THE BEHAVIORAL ROOTS OF IS SECURITY: EXPLORING KEY FACTORS OF UNETHICAL IT USE

Sutirtha Chatterjee (corresponding author)
Assistant Professor
Department of Management, Entrepreneurship, and Technology
Lee Business School
University of Nevada, Las Vegas
4505 S. Maryland Parkway
Las Vegas, Nevada 89154
Phone: (702) 895-3974
Email: Sutirtha.Chatterjee@unlv.edu; suti.chatterjee@gmail.com

Suprateek Sarker
Professor of Information Technology
McIntire School of Commerce
University of Virginia, Charlottesville, VA 22904
Chair of Technology & Information Management
Royal Holloway, University of London, UK
Phone: (434) 924-3214
Email: sarkers@virginia.edu; supra.sarker@rhul.ac.uk

Joseph S. Valacich
Eller Professor of MIS
Department of Management Information Systems
Eller College of Management
The University of Arizona
Tucson, AZ 85721-0108
Phone: (520) 621-0035
Email: valacich@email.arizona.edu

THE BEHAVIORAL ROOTS OF IS SECURITY: EXPLORING KEY FACTORS OF UNETHICAL IT USE[1]

SUTIRTHA CHATTERJEE, SUPRATEEK SARKER, AND JOSEPH S. VALACICH

SUTIRTHA CHATTERJEE is an Assistant Professor at the University of Nevada, Las Vegas. His research interests are information systems ethics, electronic markets, and mobile work its application to health care. His research has been published in *Decision Sciences Journal*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Decision Support Systems*, *Database for Advances in Information Systems*, *Information Technology and People*, and *Communications of the AIS*. He currently serves as an Associate Editor at *Information Systems Journal*, and a guest Associate Editor at *MIS Quarterly*. He also serves on the Editorial Review Boards of the *Journal of the Association for Information Systems* and *Journal of Information Technology Case and Application Research*.

SUPRATEEK SARKER is a Professor of Information Technology at the McIntire School of Commerce, University of Virginia, USA. He concurrently holds the part-time appointments of Chair of Technology & Information Management at Royal Holloway, University of London, UK, and of Visiting Distinguished Professor at Aalto University, Helsinki, Finland. Suprateek's past work has been published in outlets including the *MIS Quarterly*, *Information Systems Research*, *Journal of the AIS*, *Journal of the MIS*, *Decision Sciences*, *IEEE Transactions on Engineering Management*, *European Journal of Information Systems*, *Decision Support Systems*, *Information Systems Journal*, *Journal of Strategic Information Systems*, *Journal of Information Technology*, *ACM Transactions on MIS*, *MIS Quarterly Executive*, *Communications of the ACM*, *Communications of the AIS*, and *Journal of Academy of Marketing Science*. Suprateek is serving as a Senior Editor (Emeritus) for the *MIS Quarterly*, and as an editorial board member for journals including the *Journal of the MIS* and *IEEE Transactions on Engineering Management*. He currently serves as the Editor-in-Chief of the *Journal of the AIS*.

JOSEPH S. VALACICH is an Eller Professor of MIS in the Eller College of Management at the University of Arizona, and a Fellow of the Association for Information Systems. He received his Ph.D. degree from the University of Arizona (MIS) (1989), and M.B.A., and B.S. (computer science) degrees from the University of Montana. His primary research interests include human–computer interaction, cyber security, deception detection, technology-mediated collaboration, individual and group decision making, and e-business. His prior work has been published in numerous prestigious journals, including *MIS Quarterly*, *Information Systems Research*, *Management Science*, *Academy of Management Journal*, *Journal of MIS*, *Decision Sciences*, *Journal of the AIS*, *Communications of the ACM*, *Organizational Behavior and Human Decision Processes*, *Journal of Applied Psychology*, and many others. He is a coauthor of several leading textbooks, including *Modern Systems Analysis and Design* (7th ed.), *Information Systems Today* (6th ed.), and *Essentials of Systems Analysis and Design* (5th ed.), all published by Prentice Hall.

[1] The authors are very grateful to the SI Co-editor, Professor Robert O. Briggs, who introduced us to the exploratory research paradigm and provided helpful comments. This guidance was immensely helpful in developing this paper.

Abstract

Unethical IT use, related to activities such as hacking, software piracy, phishing, and spoofing, has become a major security concern for individuals, organizations, and society in terms of the threat to IS Security. While there is a growing body of work on this phenomenon, we notice several gaps, limitations, and inconsistencies in the literature. In order to further understand this complex phenomenon and reconcile past findings, we conduct an exploratory study to uncover the nomological network of key constructs salient to this phenomenon, and the nature of their inter-relationships. Using a scenario-based study of young adult participants, and both linear and non-linear analyses, we uncover key nuances of this phenomenon of unethical IT use. We find that unethical IT use is a complex phenomenon, often characterized by non-linear and idiosyncratic relationships between the constructs that capture it. Overall, ethical beliefs held by the individuals, along with economic, social, and technological considerations are found to be relevant to this phenomenon. In terms of practical implications, these results suggest that multiple interventions at various levels may be required to combat this growing threat to IS Security.

KEYWORDS: Unethical IT use, Ethics, Exploratory Research, Security, Nonlinear Analysis

Introduction: Focus and Motivation

In today's information age, the use of IT (information technology) is pervasive. However, with easy access to technology and the proliferation of the Internet, the possibility of using technology for unethical purposes has also increased. In many instances, unethical behaviors using IT are also illegal, and these include problems of software piracy, hacking, spoofing, and plagiarism. As an example, the Business Software Alliance [17] states that the global software piracy rate was about 42 percent in 2011; likewise, the CSI Computer Crime and Security Survey reported that in 2009, one-third of respondents' organizations experienced fraudulent phishing messages. Published academic work also highlights several instances of unethical behavior using IT [23, 31, 70]. A disturbing trend is the large scale proliferations of unethical IT use fueled by the growing worldwide popularity of personal computers and the Internet [17].

Unethical use of IT has led to serious security concerns [51] with most security violations being caused by insiders using IT in an unethical/ inappropriate manner [29], often deliberately,

and with malevolent intent [70]. Undeniably, employees using IT inappropriately present a major security threat [51]. As an illustration, published research in *Computers & Security* (a leading journal in IS security) consistently argues that unethical use (or misuse) of IT is one of the major concerns in IS security. For example, Da Veiga and Eloff [32, p. 196] note that "an organisation's approach to information security should focus on employee [unethical] behavior." Others note that one of the most popular themes of security awareness campaigns (in organizations) is related to ethical/moral use of computers and IS [63] because "people could be the weakest link in IS security" [22, p. 447]. Indeed, the misuse of computer systems "has the greatest potential for loss and damage to the employer" [132, p. 1]; this observation has been supported by others [21, 123].

Consequently, there has been an emerging consensus amongst academics about focusing on the human element in IS security research [29, 49]. Given the increasing acknowledgement by researchers in this area that there are "behavioral root[s]" of (much of) IS security problems [133, p. 212], more research is needed to develop a deeper understanding of this threat of individuals using IT unethically [107].

Pertaining to the above issue, there are noticeable gaps in the literature. *First*, prior studies in the ethical decision-making literature have often provided inconclusive or contrasting results, both in IS and general management research [31, 91, 106].[2] Specifically, Guo [49, p. 242] points out that "while this body of research has made significant contribution…, many *inconsistent findings* [have] persisted" (emphasis added). This could be due to many reasons, including sampling, statistical analyses, errors of exclusion of important factors, and divergent

[2] For example, D'Arcy et al. [33] and Herath and Rao [63] found contrasting findings regarding the relation between perceived severity of sanctions and intentions of IT misuse.

conceptualizations of security-related behaviors [30, 49]. Clearly, there is a need to reconcile such contrasting and inconclusive findings. Since prior work on unethical IT use has considered a diverse array of factors (although, not in one study), often with conflicting results, it would be fruitful to synthesize such factors into a set of "focal constructs" and relationships, by carefully balancing "richness and parsimony" [127, p. vii]. This is one of the motivations underlying our study. We also contend that our understanding of the phenomenon is constrained by the fact that prior studies have mostly focused on linear relationships and/or analyses [50]. Following prior calls [50], we remain open to the possibilities of key relationships between the variables being nonlinear, which could potentially explain some of the equivocal results found in prior studies.

Second, there is very little prior research that has sought to provide an understanding of why individuals indulge in unethical IT use from an ethical theory perspective [113]. Past work on ethical behavior in other fields has included ethical theories from philosophy when developing overarching conceptual models [36, 57], while the use of such ethical theories in research on IT use and even IS security is relatively scarce [16].[34]

Third, the role of technology in facilitating such unethical behavior largely remains to be investigated. Given that technology has spawned various ethical issues [77], along with the increasing pervasiveness of technology in our personal and professional lives, ethical ramifications of technology have much practical significance [79]. Therefore, an important focus

[3] In order to support this assertion, we conducted a search with the keywords "ethics" and "ethical" for the leading journals publishing IS research (AIS basket of six journals, IEEE-TEM, Decision Sciences Journal, and Management Science). Two other important journals which publish empirical IS Ethics research were also considered. They were *Computers & Security* and *Journal of Business Ethics*. Generally, two gaps were discovered: a lack of general development of unethical IT use based upon the theories of ethics in philosophy, and a lack of direct conceptualization of the role of technology in purporting/facilitating this unethical behavior.

[4] We also agree that there are other journals (e.g., Ethics and Information Technology) outside of the above journals which have published studies of IS Ethics. However, they are often engage in philosophical discussions of IS Ethics; due to the nature of our study, we excluded such journals from our search.

that can inform our understanding of unethical IT use is how technology plays a role in facilitating this unethical behavior, thereby having a detrimental influence on IS Security.

Given the relatively unchartered territory of studying unethical IT use, we adopt an exploratory approach to investigate this complex problem [116]. Since this phenomena is inherently linked to technical, behavioral, social, and philosophical factors [29], each is used to formulate an integrative understanding related to individuals' unethical use of IT. This will enable us to provide an intellectual foundation for better security solutions and provide an empirical foundation for future theoretical developments.

Why Exploratory Research

There are many reasons why we engage in this exploratory research, rather than the more commonly used deductive, hypotheses-testing genre. One of the primary reasons is that exploratory research is concerned with the generation of ideas [116] and "is an important approach…in the information age…because this age generates widespread change [116, p. 59]. While prior research have sought to understand the moral nature and scope of technology as well as its implications for the design of technology [39, 86, 117], this study focuses on generating ideas about the salience of *social, economic, and technological factors associated with unethical use of IT*. Thus, the goal of this study is that of exploration as well as consolidation. Specifically, the study seeks to *identify the nomological net of constructs* and their interrelationships as relevant to understanding individuals' unethical use of IT.

The importance of exploration has been observed by Stebbins [116] as well as the scholars who introduce his work by noting that "social [science] research is always (or at least should be) exploratory: a long, cumulative, choice-laden, and interest-governed process in which no single study can be definitive" (Series Editors Introduction by Van Mannen, Manning, and Miller, [116,

p. vi]). Since we are only beginning to understand this phenomenon of unethical IT use and its possible ramifications for IS security, it is reasonable to argue that exploration is an appropriate form of inquiry.

Formally, the aim of this exploratory research is to discover and describe observed variations in the phenomena of unethical IT use, their associated factors, and the contexts and conditions under which they manifest. Specifically, using the Theory of Planned Behavior or TPB [1] as a "sensitizing device" [116, p. 19]), our study explores this complex phenomenon. TPB serves as the overarching theoretical framework guiding our exploration in terms of discovering key variables (e.g., attitude and intention) as well as unearthing other variables that may be theoretically linked to these key variables (these are discussed later).

It should also be noted that "exploratory studies are those which define possible relationships in only the most general form "[where]… the researcher is not looking to "confirm" any relationships specified prior to the analysis, but instead [allowing] the method and the data to define the nature of the relationships" [12, p. 3]. In other words, there is less focus on *a-priori* expectations (i.e., formulated hypotheses) in exploratory research [13, 48] and typically *research questions* guide the empirical study [14]. True to the exploratory approach as exemplified by prior studies [53], our intention in this study is *not to engage in developing specific hypotheses*, but instead to recognize phenomena and become acquainted with the problem domain, thereby informing more specific inquiries including hypotheses development and deductive testing [89] in the future.

Philosophical Theories of Ethics

In order to analyze unethical use of IT, we first examine the concept of ethics. Guided by the universal philosophical theories of ethics, the theoretical framing of ethics can be classified

broadly into two major schools of thought: the consequentialist and deontological schools [114]. The *consequentialist school* views that the rightness (or wrongness) of an action is guided by how much consequential benefit (harm) arises out of the action [10, 82]. Alternatively, the *deontological school* of ethics views that the rightness (or wrongness) of an act is guided by certain rules in place [64]. Specifically, Kant's deontological view holds that any action is ethical if it conforms to certain overarching rules (e.g., do not lie, kill or cheat). Responding to calls made by prominent ethics scholars [85], our study draws from both the consequentialist and the deontological perspectives; using both of these ethical perspectives is beneficial given that individuals often draw from both when making decisions [119, 128].[5] We thus define unethical IT use in both deontological and consequentialist terms later in the paper.

The Theory of Planned Behavior (TPB)

The Theory of Planned Behavior [1, 9] asserts that actual behavior is most associated with the intention to carry out that behavior. The *intention to carry out a behavior* correlates with the attitude toward the behavior, the subjective norms toward the behavior, and the related perceived behavioral control. The *attitude toward the behavior* is defined as the degree of favorableness felt about the behavior [37]. Likewise, *subjective norms* refer to social pressures from friends, peers, or colleagues regarding the target behavior. *Perceived behavioral control* refers to the perception about the ability to carry out an act. TPB has been validated empirically in a variety of contexts. For instance, Armitage and Conner [2] found that the predictions of TPB held within 185 separate studies, in various domains and contexts. Thus, TPB is a powerful and robust theoretical framework for predicting human intentions and behavior, including unethical

[5] While apparently we are integrating incompatible philosophical positions, in reality, that is not the case. Rather we intend to report whether, under the conditions of our study, these positions are relevant or not.

behavior [19]. As such, TPB (or the Theory of Reasoned Action, from which TPB evolved) has often been used as a theoretical framework when investigating cases of unethical use of IT [7, 69, 94]. Although prior ethics-related work has built on a TPB framework, no known studies have utilized technology's facilitating role (among others) within the context of TPB.

It is important to note that the TPB is not a normative or judgmental theory [25]. That is, it explains why an individual engages in certain behaviors, as opposed to providing a normative justification of why certain acts *should* be committed. However, it should also be noted that while TPB is not normative, it can be used to understand behavior that is already defined and understood (as ethical or unethical) in terms of the above ethical perspectives [27].

Economics of Unethical IT Use

Our integrative model also draws upon the existing literature on Transaction Cost Economics (TCE) [129]. TCE investigates how certain basic characteristics of transactions lead to the diverse organizational arrangements that govern business exchanges in a market economy [62]. While TCE has most commonly been applied at the organization or industry levels, it has also been applied to other domains such as marriage [121], or business-to-consumer relationships [33]. Williamson's [130] conception of TCE, grounded on key assumptions about human behavior, has been broadly applied to a variety of human behavioral and decision making contexts [102, 130].

One of the key (and widely used) assumptions of TCE is *opportunism*, which is regarded as a universal human attribute [102]. This attribute of opportunism appears to be especially relevant in ethical contexts, as unethical behavior and opportunism are conceptually very similar [65]. Opportunism is the assumption that if a person is provided with an opportunity, s/he may unscrupulously seek her/his own self-interests [102]. Williamson [129, p. 47] defined

opportunism as "self-interest seeking with guile," suggesting that it includes such behaviors as lying and cheating. Opportunism is a fundamental assumption about human nature [102] and can be mitigated by having proper safeguards and controls, such as monitoring and sanctions for behaving opportunistically [131]. The concept of opportunism thus has a strong logical link with unethical behavior. Unethical use of IT can be framed as arising from opportunism, which can serve as a powerful lens through which we can understand an individual's intention to use IT unethically, especially in the presence (or absence) of existing sanctions and controls.

Defining Unethical IT Use

Mason [78] defined *privacy*, *accuracy*, *property*, and *access* (henceforth PAPA) as four ethical issues of the information age. Mason [78, p. 5] explains each of these issues as follows:

- **P**rivacy: "What information about one's self or one's associations must a person reveal to others, under what conditions and with what safeguards? What things can people keep to themselves and not be forced to reveal to others?" Privacy can be best understood as the concern with what information must one disclose and how best to protect that information [95]. Privacy can be exercised by individuals as the right to control their information, maintain confidentiality, and reduce invasiveness by others [38, 81].
- **A**ccuracy: "Who is responsible for the authenticity, fidelity, and accuracy of information? Similarly, who is to be held accountable for errors in information and how is the injured party to be made whole?" Accuracy can be understood to be concerned with the veracity of information that we receive, send, and even modify [93].
- **P**roperty: "Who owns information? What are the just and fair prices for its exchange? Who owns the channels, especially the airways, through which information is transmitted? How should access to this scarce resource be allocated?" Property can be understood as the

concept related to the ownership of information (as well as information goods) and the ability to determine compensation based on that ownership [95].

- **A**ccessibility: "What information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards?" Accessibility refers to the ability of an individual to gain access to information and the safeguards in place to ensure that the information is not compromised [95].

Drawing upon Mason's views, unethical use of IT can thus be defined as: *The willful violation - by any individual, group, or organization - of privacy, and/or property, and/or accuracy, and/or access - with respect to information/information goods residing within or part of an information system, owned/controlled by any other individual, group, or organization.* Here the violation can be understood as causing harm (a consequentialist perspective, considering bad outcomes like financial loss) as well as a deontological perspective (e.g. desecration of one's right to control one's own information). All commonly known forms of unethical IT use that threaten security, such as hacking, spoofing, and phishing, fall within the scope of this definition. This definition is also consistent with deontological and consequentialist perspectives.

It should be noted here that our conception of unethical IT use is informed by the above ethical notions in philosophy. Within this view, an act is unethical if it is in violation of the consequentialist and/or the deontological perspective, and does not consider the individual's subjective perspective. As an example, a person may feel justified pirating a piece of software in order to meet an important project deadline, but the fact that his/her behavior violates the consequentialist and/or the deontological perspective implies that s/he is still using IT in an unethical manner from the perspective of these theories.

Building on prior literature, we now formulate an exploratory model of unethical IT use. Note that the variable of focus, *Intention to Use IT Unethically*, is not actual unethical IT use. Intention has often been a regarded as a surrogate variable for behavior in past IS research (e.g., [94]). Given the nature of study and the difficulty of observing and measuring actual ethical/unethical behavior, concentrating on the factors that may (directly or indirectly) be related to intention to use IT unethically was our goal. Overall, our model contends and explores whether Intention of Unethical IT Use is associated with the Attitude toward Unethical IT Use, Subjective Norms toward Unethical IT Use, and Perceived Behavioral Control of Unethical IT Use. It also explores whether these factors, in turn, are related to other ethical, social, economic and technological factors. The following section develops this exploratory model in the form of *research questions* which guide the future empirical exploration. Each research question is developed based on arguments that point to a meaningful association between the variables captured in the research question.

Developing the Exploratory Model

Attitude toward Unethical IT Use

Fishbein and Ajzen [37] define attitude toward an act as the degree to which a person is favorable or unfavorable about the act. In our case, attitude toward unethical IT use is defined as the degree of favorableness toward the violation of PAPA (Privacy, Accuracy, Property, and Access) for any individual, group, or organization. According to the Theory of Planned Behavior [1], attitude is strongly associated with intention, and we can argue that a strong attitude in favor of unethical use of IT would be associated with a stronger intention toward unethical use of IT. Thus, we propose our first research question:

RQ1. What is the relationship between attitude toward unethical IT use and intention toward unethical IT use under the conditions in this study?

Beliefs about Information Technology

According to the TPB, attitudes are related to beliefs. Investigating attitude toward *unethical* IT use naturally points to the need to uncover *ethical* beliefs that could be argued to be related to such (un)ethical attitudes. Given our focus on unethical IT use, two kinds of (ethical) beliefs appear particularly relevant; one pertaining to a general understanding of technology and the second pertaining to the nature of the act. We discuss the salience of ethical beliefs pertaining to a general understanding about technology in this sub-section. This is followed by an examination of the ethical beliefs about the nature of the act.

Moor [85] argues that in order to develop a theoretical treatment of ethical issues related to Information Technology (IT), there is a need to consider both the deontological and consequentialist perspectives of ethics, a view that has also received support from others [119]. Building on this perspective, we examine two technology-related ethical beliefs that can be viewed from each of these ethical perspectives: technological idealism and technological relativism. Both these beliefs build upon two concepts (idealism and relativism) widely used in prior ethics research.

Forsyth [41] argues that ethical beliefs are of two distinct types that are essentially orthogonal to each other (as discussed by Forsyth), namely, idealism and relativism. Drawing from the consequentialist perspective of ethics, the concept of technological idealism builds upon Forsyth's [41] general concept of idealism, which informs an individual's ethical belief regarding any moral issue. Idealism is defined as the belief that one should not harm others [41]. Adapting this notion, we define technological idealism as *an individual's belief that technology*

should not be used to harm anyone. Inherently, as is evident in its definition, technological idealism draws upon a consequential perspective about technology, and is informed by the notion that any technology-related action should maximize the (good) consequences.

Typically, using IT unethically increases the likelihood of causing harm to others. As a case in point, unethical behaviors such as digital piracy result in harm by decreasing an organization's revenues. Hence, an individual who subscribes to the belief that technology should not be used to harm others, would find digital piracy less favorable (attitude). Hence, we can argue that individuals having a high level of technological idealism would tend to have a negative attitude toward unethical use of IT. Thus we explore:

RQ2. Is technological idealism negatively associated with attitude toward unethical IT use?

Orthogonal to idealism, relativism, is the notion that individuals will not conform to a uniform code of conduct when developing a moral attitude toward an ethical action. As such, technological relativism reflects *an individual's position that using technology should not necessarily conform to any codes or rules,* and that ethical attitudes should be based on the situational context [99]. For example, studies have found that the ethical acceptability of the same act differs across cultures (e.g., [58]).

The concept of relativism is associated with the deontological view because individuals who are low on relativism are essentially deontologists who believe that technology should be used in a way that conforms to various rules in place [68]. For example, a staunch deontologist would argue that the norms of behavior for IT use (e.g., the ACM Code of Ethics) should be strictly followed, irrespective of the situation [68]. On the other hand, individuals who are not staunch deontologists (i.e., who are high on technological relativism, and thus understand if an act is

unethical based on the surrounding context), are much more likely to have a less negative (or a more positive attitude) toward using IT in ways that may be seen as unethical by deontologists. Hence, we explore:

RQ3. Is technological relativism positively associated with attitude toward unethical IT use?

Moral Intensity

Beliefs about how technology should be used are not the only factors related to attitude formation. Another ethical belief that is relevant is the nature of the act itself. Existing literature has considered this belief as the *moral intensity* of an act, which is an extremely important factor in ethical decision-making, and reflects how the *context* is related to ethical decision making processes [61]. If the moral intensity of a situation is perceived as low, individuals will be less likely to view the situation as having ethical implications [111].

Moral intensity of an act reflects an inherent consequentialist perspective, where the extent of harm the proposed action will bring about is paramount. For example, erroneously changing an individual's medical dosage electronically would likely be of greater moral intensity than copying pirated software from a peer. In other words, a situation of unethical IT use with a relatively high moral intensity would be associated with lower degree of favorableness toward this act. This logic follows along the same line of reasoning as technological idealism, where we contend that individuals' beliefs that technology should not be used for resulting harm, would be associated with lower attitudes toward unethical use of IT. Similarly, individual beliefs that the act itself would result in a greater harm (i.e., the moral intensity is high), should arguably be associated with lower attitude toward unethical use of IT. Hence, we explore:

RQ4. Is moral intensity negatively associated with attitude toward unethical IT use?

Lack of Punishment Severity

Unethically using IT (in order to serve one's own interests) relates to opportunism [106]. Opportunistic behavior positively correlates to the benefits from the behavior [103] and is negatively associated with any related sanctions [44]. Such sanctions could potentially assume different forms, including financial penalties or jail time [94]. In other words, the overall gain perception from committing an act is positively related to the perceived lack of repercussions (e.g., punishment) for committing the act. Consequently, the overall gain of committing any act can be understood to be a cost-benefit tradeoff. Thus, the overall gain perceptions are positively associated with an individual's perceptions of lesser punishment for an act (i.e., lower costs). This suggests the following relationship to explore:

RQ5. Is perceived lack of punishment severity for unethical IT use positively associated with perceived overall gain from unethical IT use?

Overall Gain

As argued earlier, unethical use of IT is often a case of opportunism and hence the consideration of the gain from committing an act is important. Likewise, criminal behavior has often been studied from a rational angle which factors in how much of overall gain individuals perceive from a certain behavior [80]. Opportunism assumes that human beings are essentially geared toward maximizing their self-interest [109]. In other words, human beings are essentially rationalists, inherently trying to maximize their personal gain. Consequently, prior research has found that perceptions of overall rewards encourage individuals to engage in unethical behavior [108].

According to TCE and Williamson's [129] conception of unethical behavior, we can therefore argue that opportunistic behavior is more likely to be associated with higher overall

(perceived) gain from the behavior (for whatever reasons, e.g., due to the existence of low sanctions). Specifically, higher levels of overall gain perceptions are associated with higher intentions of behaving unethically. Drawing on this, we explore:

RQ6a. Is perceived overall gain from unethical IT use positively associated with intention toward unethical IT use?

It should be noted that this perceived overall gain by individuals will not only be associated with their intentions, but also their attitudes toward unethical IT use. Specifically in the case of software piracy, Moores and Chang [88] argue that attitudes are associated not only with behavioral beliefs (i.e., idealism, relativism, and moral intensity in our model), but also outcome expectations. In the context of our study, outcome expectations refer to the overall gain that the individual may perceive from the unethical use of IT. After all, it seems logical that the extent of positive outcomes from an act can be argued to be associated with the degree of favorableness (attitude) toward that act [94]. Hence, we explore:

RQ6b. Is perceived overall gain from unethical IT use positively associated with attitude toward unethical IT use?

Subjective Norms

Kuo and Hsu [67, p. 304] define subjective norms as the "desire to conform to others: confirm what others do, do what others do." Subjective norms therefore refer to the social evaluation of the behavior an individual engages in. According to the TPB, subjective norms are strong predictors of an individual's intention to act. While attitudes are primarily predispositions [135], subjective norms vary by the reference group and represent the social understanding of ethicality. Subjective norms can therefore be understood to be the acceptability of an individual's act by people surrounding the individual (e.g., peers, friends, authorities, etc.). Thus, an

individual moving from one social context to another would likely find different subjective norms. Given that subjective norms have been found to be strongly associated with behavioral intention, we explore:

RQ7. Are Subjective norms toward unethical IT use positively associated with intention toward unethical IT use?

Perceived Behavioral Control

TPB argues that the perceived behavioral control is an important consideration when predicting behavior [1], reflecting an individual's perception about the ability to carry out an act [1]. TPB posits that in order to intend and carry out an act, an individual should also perceive that s/he has the capability to do so. In the context of unethical IT use, it implies that the individual perceives that s/he has the capability to use IT unethically. Empirically, perceived behavioral control of performing software piracy (a typical unethical IT use) has been found to be positively correlated to intention to engage in software piracy [94]. Hence, we explore:

RQ8. Is perceived behavioral control of unethical IT use positively associated with intention toward unethical IT use?

Relation between Technology and Unethical Behavior

Technology is often viewed as a double edged-sword, introducing both benefits and challenges; such challenges include unethical behavior [77]. For example, technology can facilitate unethical acts [18]. Likewise, Zhou et al. [134] contend that computer-mediated communication brings with it newer possibilities of deceptive and other undesirable behaviors. For instance, researchers have observed that socially unacceptable behaviors (such as flaming) may often occur more frequently in computer-mediated groups due to the anonymity provided by

technology [100]. Consequently, it can be argued that technology can facilitate unethical (e.g., deceptive) behavior due to its unique properties [75].

Taylor and Todd [118] proposed three key factors in perceived behavioral control of any action, namely resource facilitation, technology facilitation, and computer self-efficacy. These factors are directly relevant to our conceptualization of how technology can be associated with unethical behavior and are examined next.

Resource Facilitation: Non-Traceability

Traceability refers to the tracking of an individual's use of technology through the use of audit trails, session logs, or other technologies. The lack of traceability is thus closely linked to anonymity, which has been argued to be an important implication of technology use [60, 124]. Anonymity reflects an inability to understand the true identity of an individual, possibly leading to "personal denial of responsibility" [52, p. 257]. Such lack of traceability breeds the threat of opportunism [33], and the deindividuation literature [35, 135] portrays anonymity to be a key factor of unethical and antisocial behavior. This suggests that an individual who inherently perceives that the technology provides non-traceability of his/her act, will also perceive more behavioral control in carrying out the act due to the diminished likelihood of future repercussions. Thus, we explore:

RQ9a. Is perceived non-traceability provided by technology positively associated with perceived behavioral control of unethical IT use?

We contend that, apart from being an antecedent of perceived behavioral control, the construct of non-traceability acquires additional significance in our theorization. Traceability, in our context, can be compared to the concept of punishment certainty that has been discussed in prior IS literature, especially with respect to software piracy [54, 94]. Based on Peace et al. [94],

we can conceptualize punishment certainty as the likelihood of being identified and caught for any unethical behavior using IT. Conversely, non-traceability offered by the technology can be conceptualized as the diminished likelihood of identification and punishment, since the technology itself does not promote such identifying mechanisms. Also, punishment certainty (interpreted in our context as traceability) significantly correlates with the expected outcome of an act [94]; i.e., on the perceived overall gain from unethical IT use. Hence, we explore:

RQ9b. Is perceived non-traceability provided by technology positively associated with perceived overall gain from unethical IT use?

Technological Facilitation

Arguably, the inherent interconnected nature of modern IT provides increased opportunities for unethical behavior. For instance, whether it is copying or distributing illegal software [24], the proliferation of viruses [56], or an attack by worms [6], the interconnectedness of the technology facilitates many forms of unethical behavior. Likewise, individuals perceptions that the technology provides such facilitating attributes for carrying out an unethical action would also be associated with their increased behavioral control regarding the use of the technology (for the unethical act). Thus we explore:

RQ10: Is perceived technological facilitation for unethical IT use positively associated with perceived behavioral control of unethical IT use?

Computer Self-Efficacy

In general, computer self-efficacy reflects how individuals perceive their ability to use computers [72]. Prior literature has observed that such efficacy is salient in ethical contexts [106]. Thus, if individuals perceive a greater amount of self-efficacy in handling computers, then the perceived behavioral control of their unethical IT use would also likely increase. Unethical

acts using IT typically require some level of IT skills. Consequently, a novice in computer technology, without sufficient confidence regarding his/her skills, is less likely to intend to carry out an unethical act using IT, and vice versa. Thus:

RQ11: Is computer self-efficacy positively associated with perceived behavioral control of unethical IT use?

Role of Past Behavior

Prior researchers have argued that prior behavior is associated with our current judgments. For example, Gerber et al. [43, p. 540] note that "one's pattern of behavior itself has an independent effect on subsequent conduct." With respect to ethical issues, it is probably more pertinent. In fact, as Gerber et al. [43] note, Aristotle, in his conception of ethics, noted that past behavior paved the way for subsequent ethical judgment and intentions. This view has especially been supported in the case of software piracy where many researchers have argued that the habit of software piracy contributes to continued software piracy [71, 87]. In fact, in a recent study of digital piracy, it was noted that past behavior was the most important factor associated with digital piracy intention [26]. In sum, past behavior strongly correlates to future intentions [25]. Hence we explore:

RQ12: Does extent of past behavior (experience) with respect to unethical IT use associate with intention toward unethical IT use?

Research Methodology

Research Approach

Given the inherent difficulty of studying actual ethical behavior (e.g., due to issues such as violation of privacy and social desirability), a scenario-based study was used to explore our research questions. In such studies, an ethical scenario is distributed to participants who are

asked to "role-play" and "behave as if he [or she] were a particular person in a particular situation" [4, p. 26]. Following that, the participants answer the questionnaire administered to them. The scenario-based approach has been used in prior studies dealing with ethical issues related to IT [7, 119], allowing "researchers to present concrete decision-making situations that approximate real-life situations" [8, p. 473]. One specific advantage of scenario-based approaches is that the problems of social desirability bias are lessened. This is because subjects are not often "fully attentive to the manipulation" [125, p. 506]; consequently, prior research has often used the scenario-based approach to investigate socially unacceptable behavior [59, 73].

Similar to a majority of the previous related studies, we too utilized undergraduate student participants (for an extended list of such studies, see [71]). Notably students (within the context of an educational institution) serve as an ideal *starting* point for our exploration of unethical IT use because of the following reasons. Majority of the security breaches since 2005 occurred in educational institutions [5]; similarly from February '05 to March 2006, Privacy Rights Clearinghouse assessed that almost half of the security violations reported were related to higher education institutions [92]. Also, students who are familiar with computers commit significantly more abuse [11, 28]. Given the high technological efficacy of today's undergraduate students, they seem to be a relevant sample to explore the factors related to unethical IT use.

It was also deemed that the use of undergraduate student participants in this particular context is justifiable because they are future organizational members, and future developers or users of IT. Also, the ethical scenarios for this investigation were developed to be highly relevant to this population (e.g., [74], Pew Internet and American Life Project).

Ethical Scenario Cases

Two base scenarios were utilized that reflected two distinct unethical behaviors using IT: 1) an incident of illegal downloading of music, adapted from Sarker et al. [106] and, 2) an incident of unauthorized grade changing in a professor's online grade book. These two scenarios were chosen because of their immediate relevance to the study's sample population.[6] In addition to relevance, these case scenarios were designed to exemplify a strong manipulation of the moral intensity construct, with downloading reflecting a lower moral intensity situation and grade changing a higher moral intensity situation. Both base scenarios were modified to further manipulate the exogenous variables of non-traceability and lack of punishment severity on two levels (HI vs. LO) (see Appendix B), thereby resulting in 8 case versions. Thus, a 2 X 2 X 2 between subjects design, utilizing 493 usable questionnaires, was used to explore the RQs.

Procedure and Instrument

The study was conducted in a computer lab and each subject had access to a computer. Participants were given a handout with instructions and the specific case description assigned to them, based on random assignment.[7] Subjects were instructed to go to a specified URL and carefully read the study overview, the IRB statement, and the consent statement before engaging in the study. The study administrator also briefed them and answered any questions they had; subjects were assured of complete anonymity. Subjects then read their assigned case, answered the questionnaire, and were released.

---

[6] Consistent with the literature (e.g., [116]), illegal and unethical are synonymous within the context of this study. However, we acknowledge that there may be cases where the two are not necessarily identical.

[7] Note that in order to reduce possibilities of order effects and fatigue, and sensitization by repeated exposure to the instrument within a single study session, each subject was assigned only one case version (out of the 8 possible versions)

Measures in this study used a 7-point Likert scale, strongly disagree (1) - strongly agree (7), which were adapted from literature and subjected to pilot testing. *Technological idealism and relativism* were adapted from the work of Forsyth [41]; *moral intensity* from [110, 111]; *subjective norms* from [94]; *non-traceability* from [96]; *attitude, intention, and lack of punishment severity* from [94]; *perceived behavioral control* from [118]; and *computer self-efficacy* from [76]. Finally, the items for *technological facilitation* were developed for this study. Please see Appendix A, Table A1 for the items.[8]

Empirical Analysis

Measurement Model

Three variables were manipulated through the various case scenarios: moral intensity, non-traceability afforded by the technology, and the lack of punishment severity as the repercussion for the act. Manipulation checks were conducted to ensure successful manipulations.

Warp PLS software version 3.0 was used for analyzing the data, especially due to its ability to handle both linear and nonlinear relationships [50]. We use PLS because it is focused on exploratory, theory-building exercises rather than assessing the appropriateness or fit of any overarching theoretical framework (e.g., as with traditional CB-SEM).

In PLS, the measurement model involves analyzing reliability, convergent validity, and discriminant validity [40]. In our study, the composite reliabilities (ranging from 0.879 to 0.974) were all higher than the recommended threshold, thus ensuring that our instrument was reliable [90]. Convergent validity "is shown when t-values of the Outer Model Loadings are above 1.96" [42, p. 97]. This was satisfied by all items, thereby demonstrating adequate convergent validity.

[8] It should be noted that other than technological idealism and relativism, and computer self-efficacy (which are independent of the case scenario context), each subject was asked to answer all the items with reference to the specific case scenario variation that the subject was assigned to.

Discriminant validity was assessed by: 1) confirming that the loadings of the items on their respective theoretical constructs were much higher that their (items') loadings on the other theoretical constructs and, 2) confirming that the square root of the AVE for each construct was much greater than the correlation between any pair of latent constructs [42]. The loadings of items on their respective constructs were much higher than their loadings on other constructs and satisfy the usually recommended value of 0.7 [90]. For the second condition, we examined the square root of the AVE for each construct and compared it to the correlation between any two constructs and noted that the former was much greater than the latter. Also, from Table A2 in Appendix A, the AVE scores for all constructs were higher than the recommended value of 0.5 [40]. Thus, both conditions for discriminant validity was also met.

Structural Model, Results, and Discussion

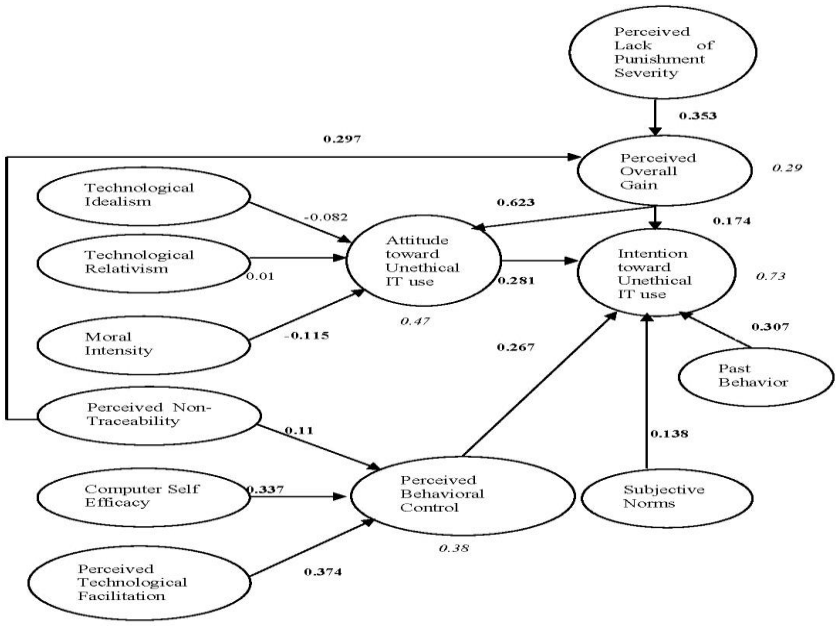

Figure 1. The Structural Model

We explore the structural model in two ways - one by investigating linear relationships between the variables (see Figure 1) and two, by investigating nonlinear relationships between

the variables (Appendix C). Recall that we proposed theory-driven research questions in the spirit of exploratory research, and do not explicitly theorize about the nature of the relationships (i.e., linear or nonlinear). We emphasize that, true to the spirit of exploratory research, the directional arrows in Figure 1 should not be construed as causal predictions but rather tendencies that are useful in explaining data, "but are not wholly predictive for future situations" [126, p. 79]. In other words, the directions of arrows do not necessarily mean that one construct acts as a causal determinant of another; rather it should be inferred that one construct can be enabled in the presence of another, and this enabling may be contingent upon other factors [115].

The exploratory paradigm allows us the freedom to explore both linear and nonlinear relationships, and consequently gain a more nuanced view of the phenomenon of unethical IT use. The reason for offering both types of relationships is that while nonlinear relationships provide more interesting insights, linear analyses are still often preferred especially when the theory does not specifically predict a nonlinear relationship [66]. So, we still offer the linear insights apart from nonlinear ones.

Linear Relationships

We briefly summarize and discuss the linear associations here (see Table 1). Technological idealism had a weak relation with attitude ($p=0.07$). We found that ethical beliefs about the act (moral intensity) are associated with attitude toward unethical IT use. Perceptions of overall gain also strongly correlate with attitude toward unethical IT use. Likewise, attitude toward unethical IT use, subjective norms, perceived behavioral control, and overall gain perceived from committing the act, are all strongly associated with intention toward unethical IT use. Furthermore, overall perceptions of gain were strongly correlated to perceptions of punishment and non-traceability of the act. Perceived behavioral control is associated with the technological

facilitation of the unethical act, the general computer self-efficacy of the individual, and the lack of traceability provided by the technology. Finally, past behavior was associated with the intention toward unethical IT use.

RQ #	Linear Association	Significance
1	Attitude in favor of unethical IT use WITH Intention in favor of unethical IT use (+)	p<0.001
2	Technological Idealism WITH Attitude in favor of unethical IT use (-)	Weakly significant (p=0.07)
3	Technological Relativism WITH Attitude in favor of unethical IT use (+)	Non-significant
4	Moral Intensity WITH Attitude in favor of unethical IT use (-)	p<0.005
5	Lack of Punishment Severity WITH Overall Gain (+)	p<0.001
6a	Overall Gain WITH Intention in favor of unethical IT use (+)	p<0.001
6b	Overall Gain WITH Attitude in favor of unethical IT use (+)	p<0.001
7	Subjective Norms WITH Intention in favor of unethical IT use (+)	p<0.001
8	Perceived Behavioral Control WITH Intention in favor of unethical IT use (+)	p<0.001
9a	Non-traceability WITH Perceived Behavioral Control (+)	p<0.001
9b	Non-traceability WITH Overall gain (+)	P<0.001
10	Technological facilitation WITH Perceived Behavioral Control (+)	p<0.001
11	Computer Self efficacy WITH Perceived Behavioral Control (+)	p<0.001
12	Past Behavior WITH Intention in favor of unethical IT use (+)	P<0.001

Table 1. Linear Association results

Starting with the ethical beliefs, we discuss the implications of each of the (linear) results below. Technological idealism is the view that one should use technology so as to maximize the good consequences and reduce the harmful consequences from using it. Our results show that such consequences of technology use were of low concern to our subjects when they were interacting with technology. This is also possibly due to de-individuation and de-humanization effects of technology, a notion alluded to in prior research [97, 98].

We note that technological relativism has no relationship with attitude toward unethical IT use. Technological relativists are ones who do not believe in standard rules or codes for using technology. A deontologist (one who scores low on the technological relativism scale), on the other hand, is one who believes in such standard rules or codes. Therefore, if deontologists had strong inhibitions against unethical IT use, it would have been reflected in a strong relation between technological relativism and attitude toward unethical IT use.

The nature of the act itself (i.e., the moral intensity) has strong salience with the ethical attitude regarding the act. We contend that while considering the moral intensity of the act, individuals are *forced* to contemplate the gravity (and thus, the immediate harm) of their act.

As expected, attitude toward unethical IT use, perceived behavioral control, and subjective norms, were significantly related to intention toward unethical IT use. However, subjective norms had a weaker relation with intention than both behavioral control and attitude. This result implies that unethical use of IT was viewed as more of an individualist act, possibly due to the lower social presence and anonymity that IT often induces [101].

We also found that the lack of punishment severity and lack of traceability were strongly related to overall gain, and, overall gain is strongly linked to intention of unethical IT use. This implies that economic concerns were of utmost importance in considerations of unethical IT use in our study. It also reiterates the notion that human beings are probably, by nature, opportunistic (a notion forwarded by many noted economists such as [129]). In our case scenarios, for example, the punishment and traceability perceptions were manipulated (e.g., a warning vs. the expulsion from the university, and the existence vs. non-existence of log and audit files, respectively), and our results show that individuals were more inclined to commit an unethical act (i.e., are opportunistic) if there were little or no repercussions (e.g., only a warning), or if there were little or no possibility of being detected (e.g., no audit files for traceability purposes).

Our results also indicate that perceived behavioral control is salient to intention toward unethical IT use. Further, perceived behavioral control is itself influenced by the individual's perceptions about their ability to use and manipulate IT. This cautions us that greater proficiency in IT not only leads to benefits, but can also be associated with unethical use of IT.

Technological factors (e.g., non-traceability) were found to be significantly related to perceived behavioral control of unethical IT use. The results show that individuals perceive greater control over unethical IT use when the traceability is low. Again, our results show that individuals who believe technology facilitates unethical use of IT, report greater perceived behavioral control of the unethical act. Both these observations indicate that technology itself can act as an important factor in unethical IT use, one of the foundational premises of this research.

Finally, prior behavior was significantly related to unethical IT use. This reinforces the notion that our past unethical IT use patterns form a habit which relates to our future intentions to act in a similar manner. This is consistent with prior research such as Limayem et al. [71].

Nonlinear relationships

It is interesting to note that all the relationships, barring the one between SN (subjective norms) and intent, were nonlinear, as shown in the Figures C1-C14 (Appendix C). First, we see that the relationship between attitude and intention is linear for most parts, as also significant at all best-fitting curve segments, but tends to be asymptotic at the ends. This implies that except in extreme situations ("the ends"), intentions and attitude toward unethical IT use share a strong, linear, positive correlation. This linear relationship is somewhat expected, and is consistent with TPB. However, the nonlinearity of the relationship when attitudes/intentions are strong or weak implies that very strong or weak attitudes do not necessarily relate to equally strong or weak intentions. This can be partly understood in terms of a new concept called attitudinal ambivalence [3], which is the simultaneous exhibition of both positive and negative attitude toward the attitude object, and extends the conception of attitude as a one-dimensional construct (ibid). In our context, this would translate to a simultaneous positive and negative attitude toward unethical IT use. We believe the nonlinear relationship between attitude and intention could be

due to the fact that one of the positive or negative attitudes dominates in extreme cases. However, this obviously needs to be investigated further by future studies.

The negative relationship between idealism and attitude is also asymptotic toward the ends. At the edges, the idealism has a strong significant relationship with attitude. However, in the middle, attitude does not change with increasing idealism. In other words, idealism is related to attitude only when the idealism perceptions are either very strong or very weak. This probably explains why idealism did not have a strong linear relationship with attitude. Most likely, the relationship of technological idealism with attitude is at least partially explained by the difficulty of determining, *a-priori*, the consequence of engaging in a particular act using IT, thus rendering consequentialism less robust for predicting ethical decision making [20], especially in the middle part of the graph where idealism or attitude are not strong enough.

Relativism also has a linear relationship with attitude toward unethical IT use, but only when the relativism is small. However, at high levels of relativism, the link between relativism and attitude becomes tenuous and non-significant. This is possibly because highly relativist individuals may potentially consider *other* contingent factors and not rely only on their ethical beliefs regarding technology. The lack of this effect may imply that low deontological norms become irrelevant in the context of unethical IT use, due to the fact that IT often introduces "moral vacuum" [112, p. 280]. Indeed, our results are partly supported by prior observations on the limitations of deontology to address ethical issues related to IT [39, 112].

Moral Intensity and attitude toward unethical IT use have a strong, consistently negative curvilinear relationship; this becomes more prominent at the edges where moral intensity is high or low. In other words, it shows that moral intensity is an important factor associated with attitude. In our case scenarios, for example, individuals were more favorable toward the illegal

download of music (lower moral intensity) as compared to an unauthorized change to a professor's online gradebook (higher moral intensity). High moral intensity almost always acts as a strong deterrent, while low moral intensity almost certainly acts as a strong promoter of positive attitude toward unethical use of IT.

The relation between punishment severity and overall gain also follows a similar pattern, with gain perceptions become even more prominent when punishments are either very high, or negligibly low. Overall gain also has a nearly linear relationship with intention when it is low. But the relationship becomes weaker as perceptions of gain increase. This is a surprising finding, which tells us that high perceptions of overall gain, while being a significant factor, may not always be the salient issue related to unethical intentions. A very similar pattern is also observed for the relationship between overall gain and attitude. In other words, economic gains are not always the significant motivating cause behind unethical behavior. These findings are counter-intuitive, especially because financial and other gains have been considered strong influencers of unethical behavior in prior research [55]. One possible explanation for this is that unethical behavior may not always be pre-planned and could be impulsive, sometimes resulting from a lack of self-control [46]. In impulsive behavior, purely rational calculations (which are well-thought out) may often be absent [105].

Subjective norms and intention have a linear relationship, which means that considerations of referent others remains consistently salient in unethical behavior. The relationship between perceived behavioral control (PBC) and intention gets a little weaker as PBC increases; this might imply that unethical behavior is not solely related to control perceptions -- unethical use of IT requires some control, but beyond a certain level, increase of control perceptions start to matter relatively less.

Non-traceability has an interesting relationship with PBC. The relationship is very weak at low levels of non-traceability. But at high levels of non-traceability (or very low traceability), PBC increases dramatically and significantly. The relationship between non-traceability and overall gain is always strong; however, it again increases dramatically as non-traceability increases. In other words, expectations of gain are associated with strong perceptions that the technology does not provide traceability for unethical behavior.

The role of technology was captured because in our case scenarios, we manipulated the traceability offered by technology. Subject responses to both these manipulations indicate that technology can be a salient factor in unethical IT use, one of the premises of this research. PBC largely increases linearly with technological facilitation; however, at very high levels of technology facilitation, PBC increases quite dramatically. Efficacy does not matter at low levels (low efficacy would make PBC irrelevant), but after that PBC increases linearly with efficacy.

Finally, past behavior is correlated with current intentions, though the effect is somewhat more pronounced if the individual has had less experience with such behaviors. This is surprising, as habit has an important role to play in software piracy behavior [71]. One possible explanation is that unethical behavior is linked to creativity and novelty [45]. We contend that unethical behavior is more attractive if it presents a novel way to benefit in a particular situation; especially as creativity and self-esteem have been found to be positively correlated [47]. With repeated engagement in such unethical behavior, this perception of novelty likely wears off.

Based on the results discussed above, we believe that our nonlinear analyses of the relationships between the variables often illuminate interesting patterns, often very different from what linear analyses may reveal. Indeed, the results provide fertile ground for future confirmatory research, and we urge our academic colleagues to take up this exercise.

Regardless of the type of analyses (linear/nonlinear), our findings highlight two overall implications regarding unethical IT use. To reduce unethical IT use, technological controls such as surveillance and audit of IT use need to be implemented. However, greater surveillance has other ethical ramifications (e.g., loss of privacy), and consequently, administrators and policy makers need to be aware of this tension and strike a fine balance.

The second implication stems from the fact that even such controls and procedures may not still be sufficient to stop the unethical use of IT. IT can always be appropriated in a manner not consistent with its spirit or purpose [34] as it is "logically malleable" [84, 86]. So, another important implication is the development of ethically-conscious human beings, who would not be inclined to use IT unethically, irrespective of the existing controls, punishment, or even their own computer efficacy. Sound moral education and greater awareness of unethical IT use thus needs to be imparted early, probably as a part of primary and secondary socialization. This is appropriate because among college students (our sample), the propensity toward intention of unethical behavior (as indicated by their intention) was quite high.

Contribution

This research contributes to existing IS literature in a number of ways. It *is one of the first attempts to develop a relatively comprehensive, theoretical understanding of unethical IT use* based on an exploratory examination of a wide range of factors: individual, philosophical, social, economic, and technological. Following Weber's [127] call, the study seeks to balance both richness and parsimony by concentrating on the focal constructs associated with unethical IT use. We believe that the study makes an important contribution to the literature on IS ethics by incorporating factors drawn from multiple traditions within one unifying model. It also

illuminates interesting nuances (e.g., nonlinear relationships) in the relationships between the variables under consideration.

The second contribution is that it informs the arena of IS security. Instances of such unethical use of IT have become a major security concern [51]. Often, little research has investigated this phenomenon from the lens of ethical theory [113]. In order to address this existing gap, our research, grounded in the philosophical theories of ethics, *explores a general understanding of unethical IT use*. Such insights inform not only training, but also the design of organizational acceptable use policies.

Third, one of the features of our study is its engagement with nonlinear analyses. While linear analyses are more prevalent, researchers have argued that nonlinear analyses "can also generate richer models due to the broader interpretation of theory" [66, p. 823]. The findings from our nonlinear analyses thus provide richer insights into our focal phenomenon.

Finally, the study implies that technology plays a role in unethical behavior. In doing so, this research adds to the literature on IS ethics by trying to understand the moral implications of technology. While technology may inherently be amoral, the study suggests that there are certain technological characteristics that may be appropriated to aid unethical behavior.

Limitations of the Study

While case scenarios may be criticized for being unrealistic, a sizeable number of the respondents acknowledged to having undertaken an unethical act similar to the ones described in the case scenarios, indicating that they are indeed realistic. For example, 21.7% of the respondents (who were assigned the case of illegal downloading of music) responded that they had undertaken this action one or more times prior to this study. Social response bias is also a possible concern, but we followed guidelines to test for it [122] and found that it was not a

concern. Also, we empirically studied two instances of unethical IT use and our work may not be generalizable to other cases of unethical IT use. So we call for future research to subject our conceptual model to empirical testing in the context of other unethical uses of IT. Related to this issue of generalizability, the subjects were from a North American B-School context. Thus, the results of this study might mainly reflect perceptions of B-School students from North America. We therefore call upon future research to conduct more confirmatory work - especially because ours in an exploratory study - across other countries and population samples (particularly adult population) to increase the external validity of these results.

Future Research and Practice Implications

As with all exploratory research, the relationships discovered and reported under the conditions of this study may have different relationships in other contexts; so further research is warranted to reinforce (or invalidate) these findings. Future research can apply the findings to different forms of unethical IT use. Prior research has also argued that culture has a strong relation to ethical perceptions and decision-making [104]. So, it would be enlightening to empirically examine the relation between different facets of culture and unethical IT use.

Second, ours was a primarily quantitative study, and we did not capture qualitative data related to the constructs in the study. However, qualitative research often reveals additional nuances especially in the form of tensions and dialectics [120]. Therefore, undertaking a qualitative exploration of this phenomenon would be beneficial.

Finally, we feel the need for investigating unethical IT beyond just individual users. For example, Sarker et al. [106] investigate group ethical-decision making. Likewise, investigations of unethical IT use could include those by collectives such as governments and organizations.

Drawing from our discussion above, we now briefly enumerate the practical implications of this study.[9] The first implication is sensitization to ethical IT use. For example, many individuals may not be aware that downloading information goods (e.g., music, software, movies, etc.) from the web can be deemed as unethical acts. Some of our respondents acknowledged (in their comments) that they had done so before, but would not do it any further. Likewise, plagiarism from the internet (another instance of unethical IT use) may not be seriously viewed by some individuals as unethical due to lack of explicit awareness. In general, the infusion of IT often requires a reinterpretation of existing notions of (un)ethical behavior [117]. So, as a first step, organizations should clearly delineate what constitutes unethical IT use. Second, noting that unethical IT use has a strong opportunistic flavor, organizations should implement technological controls/sanctions in order to deter opportunities of unethical IT use.

Conclusion

To conclude, we hope that this study provides serious impetus to the continuing research on understanding the behavioral root to IS Security. Ethical challenges in IS have grabbed the attention of IS researchers [83]. There have been passionate calls to investigate ethical problems in IS phenomena [15] which particularly gain prominence in light of the multiple large-scale security breaches, such as those in TJ Max and Home Depot. This study uncovers interesting insights, and potentially has important implications to organizations, society, and the general economy as they all try to wrestle with the ethical challenges of the information age.

[9] These findings are correlative, not causal, and so should be used carefully. These findings will become more dependable as a cumulative body of work reports similar findings.

References

1. Ajzen, I. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50, 2 (1991), 179-211.
2. Armitage, C.J., and Conner, M. Efficacy of the Theory of Planned Behaviour: a meta-analytic review. *The British journal of social psychology* 40, 4 (2001), 471-499.
3. Armitage, C.J., and Conner, M. The effects of attitudinal ambivalence on attitude-intention-behavior relations. *Contemporary perspectives on the psychology of attitudes* (2004), 121-143.
4. Aronson, E., and Carlsmith, J.M. Experimentation in social psychology. In, Lindzey, G., and Aronson, E., (eds.), *The handbook of social psychology*, Reading, MA: Addison-Wesley, 1968, pp. 1-79.
5. Ayyagari, R., and Tyks, J. Disaster at a University: A Case Study in Information Security. *Journal of Information Technology Education*, 11 (2012).
6. Bagchi, K., and Udo, G. An Analysis of the Growth of Computer and Internet Security Breaches by *Communications of the Association for Information Systems*, 12, (2003), 684-700.
7. Banerjee, D., Cronan, T.P., and Jones, T.W. Modeling IT ethics: A study in situational ethics. *Mis Quarterly*, 22, 1 (1998), 31-60.
8. Barnett, T., Bass, K., and Brown, G. Ethical ideology and ethical judgment regarding ethical issues in business. *Journal of Business Ethics*, 13, 6 (1994), 469-480.
9. Beck, L., and Ajzen, I. Predicting dishonest actions using the theory of planned behavior. *Journal of Research in Personality*, 25, (1991), 285–301.
10. Bentham, J. An Introduction to the Principles of Morals and Legislation. New York, NY: Methuen, 1789/1970.
11. Blanke, S.J. A Study of the Contributions of Attitude, Computer Security Policy Awareness, and Computer Self-Efficacy to the Employees' Computer Abuse Intention in Business Environments. Nova Southeastern University, 2008.
12. Boudreau, M.-C., Gefen, D., and Straub, D.W. Validation in information systems research: A state-of-the-art assessment. *Mis Quarterly* (2001), 1-16.
13. Bowen, G.A. Preparing a qualitative research-based dissertation: Lessons learned. *The Qualitative Report*, 10, 2 (2005), 208-222.
14. Brady, M.K., and Robertson, C.J. Searching for a consensus on the antecedent role of service quality and satisfaction: an exploratory cross-national study. *Journal of Business Research*, 51, 1 (2001), 53-60.
15. Bryant, A., Land, F., and King, J.L. Editors' Introduction. *Journal of the Association for Information Systems*, 10, 11 (2009), 782-786.
16. Bull, C.M. A review of ethical theory in the 'upper echelons' of information systems research. *17th European Conference on Information Systems*, Verona, Italy, 2009.
17. BusinessSoftwareAlliance. 2011 BSA global software piracy study. 2012.
18. Cappel, J.J., and Windsor, J.C. Ethical decision making: A comparison of computer-supported and face-to-face group. *Journal of Business Ethics*, 28, 2 (2000), 95-107.
19. Chang, M.K. Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior. *Journal of Business Ethics*, 17, 16 (1998), 1825-1834.
20. Chatterjee, S., Sarker, S., and Fuller, M. A Deontological Approach to Designing Ethical Collaboration. *Journal of the Association for Information Systems*, 10, 3 (2009a), 138-169.

21. Chen, Y., Ramamurthy, K., and Wen, K.-W. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 29, 3 (2012), 157-188.

22. Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *computers & security*, 39 (2013), 447-459.

23. Chiou, J.-S., Huang, C.-y., and Lee, H.-h. The Antecedents of Music Piracy Attitudes and Intentions. *Journal of Business Ethics*, 57, 2 (2005), 161-174.

24. Conner, K.R., and Rumelt, R.P. Software Piracy: An Analysis of Protection Strategies. *Management Science*, 37, 2 (1991), 125-139.

25. Conner, M., and Armitage, C.J. Extending the Theory of Planned Behavior: A Review and Avenues for Further Research. *Journal of Applied Social Psychology*, 28, 15 (1998), 1429-1464.

26. Cronan, T., and Al-Rafee, S. Factors that Influence the Intention to Pirate Software and Media. *Journal of Business Ethics*, 78, 4 (2008), 527-545.

27. Cronan, T.P., and Douglas, D.E. Toward a Comprehensive Ethical Behavior Model for Information Technology. *Journal of Organizational and End User Computing*, 18, 1 (2006).

28. Cronan, T.P., Foltz, C.B., and Jones, T.W. Piracy, computer crime, and IS misuse at the university. *Communications of the ACM*, 49, 6 (2006), 84-90.

29. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. Future directions for behavioral information security research. *computers & security*, 32 (2013), 90-101.

30. D'Arcy, J., and Herath, T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20, 6 (2011), 643-658.

31. D'Arcy, J., Hovav, A., and Galletta, D. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20, 1 (2009), 79-98.

32. Da Veiga, A., and Eloff, J.H. A framework and assessment instrument for information security culture. *computers & security*, 29, 2 (2010), 196-207.

33. Datta, P., and Chatterjee, S. The economics and psychology of consumer trust in intermediaries in electronic markets: the EM-Trust Framework. *European Journal of Information Systems*, 17, 1 (2008), 12-28.

34. DeSanctis, G., and Poole, M.S. Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization science*, 5, 2 (1994), 121-147.

35. Diener, E. Deindividuation: The absence of self-awareness and self-regulation in group members. Hillsdale, NJ: Erlbaum, 1980.

36. Ferrell, O.C., and Gresham, L.G. A Contingency Framework for Understanding Ethical Decision Making in Marketing. *The Journal of Marketing*, 49, 3 (1985), 87-96.

37. Fishbein, M., and Ajzen, I. Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley, 1975.

38. Flaherty, D.H. Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States. UNC Press Books, 1989.

39. Floridi, L. Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology*, 1, 1 (1999), 37-56.

40. Fornell, C., and Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18, 1 (1981), 39-50.

41. Forsyth, D. A taxonomy of ethical ideologies. *Journal of personality and social psychology*, 39, 1 (1980), 175-184.

42. Gefen, D., and Straub, D. A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example. *Communications of the Association for Information Systems*, 16, (2005), 91-109.

43. Gerber, A.S., Green, D.P., and Shachar, R. Voting May Be Habit-Forming: Evidence from a Randomized Field Experiment. *American Journal of Political Science*, 47, 3 (2003), 540-550.

44. Ghoshal, S., and Moran, P. Bad for practice: A critique of the transaction cost theory. *Academy of Management. The Academy of Management Review*, 21, 1 (1996), 13-47.

45. Gino, F., and Ariely, D. The dark side of creativity: original thinkers can be more dishonest. *Journal of personality and social psychology*, 102, 3 (2012), 445.

46. Gino, F., Schweitzer, M.E., Mead, N.L., and Ariely, D. Unable to resist temptation: How self-control depletion promotes unethical behavior. *Organizational Behavior and Human Decision Processes*, 115, 2 (2011), 191-203.

47. Goldsmith, R.E., and Matherly, T.A. Creativity and self-esteem: A multiple operationalization validity study. *The Journal of psychology*, 122, 1 (1988), 47-56.

48. Guba, E.G., and Lincoln, Y.S. Competing paradigms in qualitative research. *Handbook of qualitative research*, 2 (1994), 163-194.

49. Guo, K.H. Security-related behavior in using information systems in the workplace: A review and synthesis. *computers & security*, 32 (2013), 242-251.

50. Guo, K.H., Yuan, Y., Archer, N.P., and Connelly, C.E. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, 28, 2 (2011), 203-236.

51. Haines, R., and Leonard, L.N.K. Individual characteristics and ethical decision-making in an IT context. *Industrial Management and Data Systems*, 107, 1 (2007), 5-20.

52. Harrington, S.J. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *Mis Quarterly*, 20, 3 (1996), 257-278.

53. Hart, S., Hogg, G., and Banerjee, M. Does the level of experience have an effect on CRM programs? Exploratory research findings. *Industrial Marketing Management*, 33, 6 (2004), 549-560.

54. Herath, T., and Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 2 (2009), 154-165.

55. Hershfield, H.E., Cohen, T.R., and Thompson, L. Short horizons and tempting situations: Lack of continuity to our future selves leads to unethical decision making and behavior. *Organizational Behavior and Human Decision Processes*, 117, 2 (2012), 298-310.

56. Householder, A., Houle, K., and Dougherty, C. Computer Attack Trends Challenge Internet Security, Security and Privacy. *Supplement to IEEE Computer* (2002), 5-7.

57. Hunt, S.D., and Vitell, S.J. A General Theory of Marketing Ethics. *Journal of Macromarketing*, 6, 1 (1986), 5-16.

58. Husted, B.W. The impact of national culture on software piracy. *Journal of Business Ethics*, 26, 3 (2000), 197-211.

59. Jasso, G. Factorial Survey Methods for Studying Beliefs and Judgments. *Sociological Methods & Research*, 34, 3 (2006), 334-423.

60. Johnson, D.G. Ethics online. Association for Computing Machinery. Communications of the ACM, 40, 1 (1997), 60-65.

61. Jones, T.M. Ethical Decision Making by Individuals in Organizations: An Issue-Contingent Model. *Academy of Management. The Academy of Management Review*, 16, 2 (1991), 366-395.

62. Joskow, P.L. Transaction Cost Economics, Antitrust Rules, and Remedies. *J Law Econ Organ*, 18, 1 (2002), 95-116.

63. Kajzer, M., D'Arcy, J., Crowell, C.R., Striegel, A., and Van Bruggen, D. An exploratory investigation of message-person congruence in information security awareness campaigns. *computers & security*, 43 (2014), 64-76.

64. Kant, I. Ethical Philosophy: Grounding for the Metaphysics of Morals (trans. James W. Ellington). Indianapolis: Hackett, 1804/1994.

65. Kelley, S.W., Skinner, S.J., and Ferrell, O.C. Opportunistic behavior in marketing research organizations. *Journal of Business Research*, 18, 4 (1989), 327-340.

66. Klein, G., Jiang, J.J., and Cheney, P. Resolving difference score issues in information systems research. *Management Information Systems Quarterly*, 33, 4 (2009), 12.

67. Kuo, F.-Y., and Hsu, M.-H. Development and validation of ethical computer self-efficacy measure: The case of softlifting. *Journal of Business Ethics*, 32, 4 (2001), 299-315.

68. Laudon, K.C. Ethical concepts and information technology. *Commun. ACM*, 38, 12 (1995), 33-39.

69. Leonard, L.N.K., and Cronan, T.P. Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences. *Journal of the Association for Information Systems*, 1, 1 (2000), 1-31.

70. Liang, H., and Xue, Y. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11, 7 (2010), 394-413.

71. Limayem, M., Khalifa, M., and Chin, W.W. Factors Motivating Software Piracy: A Longitudinal Study. *IEEE Transactions on Engineering Management*, 51, 4 (2004), 414-425.

72. Loch, K.D., and Conger, S. Evaluating ethical decision making and computer use. *Association for Computing Machinery. Communications of the ACM*, 39, 7 (1996), 74-83.

73. Lowry, P.B., Moody, G.D., Galletta, D.F., and Vance, A. The Drivers in the Use of Online Whistle-Blowing Reporting Systems. *Journal of Management Information Systems*, 30, 1 (2013), 153-190.

74. Madden, M., and Lenhart, A. Music Downloading, File Sharing and Copyright. *Pew Internet and American Life Project*: PewResearchCenter, 2003.

75. Maner, W. Unique ethical probelms in information technology. *Science and Engineering Ethics*, 2, 2 (1996), 137-154.

76. Marakas, G.M., Johnson, R.D., and Clay, P.F. The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time. *Journal of the Association for Information Systems*, 8, 1 (2007), 16–46.

77. Marshall, K.P. Has technology introduced new ethical problems? *Journal of Business Ethics*, 19, 1 (1999), 81-90.

78. Mason, R.O. Four Ethical Issues of the Information Age. *Mis Quarterly*, 10, 1 (1986), 5-12.

79. Mason, R.O. Applying ethics to information technology issues. *Commun. ACM*, 38, 12 (1995), 55-57.

80. McPheters, L.R. Criminal behavior and the Gains from Crime. *Criminology*, 14, (1976), 137-152.

81. Milberg, S.J., Smith, H.J., and Burke, S.J. Information privacy: Corporate management and national regulation. *Organization science*, 11, 1 (2000), 35-57.

82. Mill, J.S. *Utilitarianism* Indianapolis, IN: Hackett Publishing, 1861/1979.

83. Mingers, J., and Walsham, G. Toward Ethical Information Systems: The Contribution of Discourse Ethics. *Mis Quarterly*, 34, 4 (2010), 833-854.

84. Moor, J.H. What Is Computer Ethics? *Metaphilosophy*, 16, 4 (1985), 266-275.

85. Moor, J.H. Just consequentialism and computing. *Ethics and Information Technology*, 1, 1 (1999), 61-65.

86. Moor, J.H. The future of computer ethics: You ain't seen nothin' yet! *Ethics and Information Technology*, 3, 2 (2001), 89-91.

87. Moores, T.T. The effect of national culture and economic wealth on global software piracy rates. *Commun. ACM*, 46, 9 (2003), 207-215.

88. Moores, T.T., and Chang, J.C.-J. Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model. *Mis Quarterly*, 30, 1 (2006), 167-180.

89. Nunamaker Jr, J.F., Chen, M., and Purdin, T.D. Systems development in information systems research. *Journal of Management Information Systems*, 7, 3 (1990), 89-106.

90. Nunnally, J. *Psychometric Theory, 2nd Ed*. New York: McGraw Hill, 1978.

91. O'Fallon, M.J., and Butterfield, K.D. A Review of The Empirical Ethical Decision-Making Literature: 1996–2003. *Journal of Business Ethics*, 59, 4 (2005), 375-413.

92. Oblinger, D.G., and Hawkins, B.L. The myth about IT security. *Educause Review*, 41, 3 (2006), 14-15.

93. Parrish Jr, J.L. PAPA knows best: Principles for the ethical sharing of information on social networking sites. *Ethics and Information Technology*, 12, 2 (2010), 187-193.

94. Peace, A.G., Dennis, F.G., and Thong, J.Y.L. Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, 20, 1 (2003), 153-177.

95. Peslak, A.R. PAPA Revisited: A Current Empirical Study of the Mason Framework. *Journal of Computer Information Systems*, 46, 3 (2006).

96. Pinsonneault, A., and Heppel, N. Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *Journal of Management Information Systems*, 14, 3 (1997), 89-108.

97. Postmes, T., Spears, R., and Lea, M. Breaching or Building Social Boundaries?: SIDE-Effects of Computer-Mediated Communication. *Communication Research*, 25, 6 (1998), 689-715.

98. Postmes, T., Spears, R., and Lea, M. The formation of group norms in computer-mediated communication. *Human Communication Research*, 26, 3 (2000), 341-371.

99. Reidenbach, R.E., Robin, D.P., and Dawson, L. An Application and Extension of a Multidimensional Ethics Scale to Selected Marketing Practices and Marketing Groups. *Academy of Marketing Science Journal*, 19, 2 (1991), 83-92.

100. Reinig, B.A., Briggs, R.O., and Nunamaker Jr, J.F. Flaming in the electronic classroom. *Journal of Management Information Systems* (1997), 45-59.

101. Rice, R.E. Computer-mediated communication and organizational innovation. *Journal of Communication*, 37, 4 (1987), 65-94.

102. Rindfleisch, A., and Heide, J.B. Transaction Cost Analysis: Past, Present, and Future Applications. *The Journal of Marketing*, 61, 4 (1997), 30-54.

103. Riordan, M.H., and Williamson, O.E. Asset Specificity and Economic Organization. *International Journal of Industrial Organization*, 3, 4 (1985), 365-368.

104. Robertson, C., and Fadil, P.A. Ethical Decision Making in Multinational Organizations: A Culture-Based Model. *Journal of Business Ethics*, 19, (1999), 385-392.

105. Rook, D.W., and Fisher, R.J. Normative influences on impulsive buying behavior. *Journal of consumer research* (1995), 305-313.

106. Sarker, S., Sarker, S., Chatterjee, S., and Valacich, J.S. Media Effects on Group Collaboration: An Empirical Examination in an Ethical Decision-Making Context. *Decision Sciences*, 41, 4 (2010), 887-931.

107. Schultz, E.E. A framework for understanding and predicting insider attacks. *computers & security*, 21, 6 (2002), 526-531.

108. Schweitzer, M.E., Ordóñez, L., and Douma, B. Goal setting as a motivator of unethical behavior. *Academy of Management Journal*, 47, 3 (2004), 422-432.

109. Sen, A.K. Rational Fools: A Critique of the Behavioral Foundations of Economic Theory. *Philosophy and Public Affairs*, 6, 4 (1977), 317-344.

110. Singhapakdi, A., Rawwas, M.Y.A., Marta, J.K., and Ahmed, M.I. A cross-cultural study of consumer perceptions about marketing ethics. *The Journal of Consumer Marketing*, 16, 3 (1999), 257-272.

111. Singhapakdi, A., Vitell, S.J., and Kraft, K.L. Moral intensity and ethical decision-making of marketing professionals. *Journal of Business Research*, 36, 3 (1996), 245-255.

112. Siponen, M., and Vartiainen, T. Unauthorized copying of software and levels of moral development: a literature analysis and its implications for research and practice. *Information Systems Journal*, 14, 4 (2004), 387-407.

113. Siponen, M.T., and Oinas-Kukkonen, H. A Review of Information Security Issues and Respective Research Contributions. *Database for Advances in Information Systems*, 38, 1 (2007), 60-80.

114. Smith, H.J. Ethics and Information Systems: Resolving the Quandaries. *Database for Advances in Information Systems*, 33, 3 (2002), 8-22.

115. Smith, M.L. Overcoming theory-practice inconsistencies: Critical realism and information systems research. *Information and Organization*, 16, 3 (2006), 191-211.

116. Stebbins, R.A. Exploratory research in the social sciences. Sage, 2001.

117. Tavani, H.T. The state of computer ethics as a philosophical field of inquiry: Some contemporary perspectives, future projections, and current resources. *Ethics and Information Technology*, 3, 2 (2001), 97-108.

118. Taylor, S., and Todd, P.A. Understanding information technology usage: A test of competing models. *Information Systems Research*, 6, 2 (1995), 144-176.

119. Thong, J.Y.L., and Yap, C.-S. Testing an ethical decision-making theory: The case of softlifting. *Journal of Management Information Systems*, 15, 1 (1998), 213-227.

120. Trauth, E.M., and Jessup, L.M. Understanding computer-mediated discussions: positivist and interpretive analyses of group support system use. *Mis Quarterly* (2000), 43-79.

121. Treas. Money in the bank: Transaction costs and the economic organization of marriage. *American Sociological Review*, 58, 5 (1993), 723-734.

122. Turel, O., Serenko, A., and Giles, P. Integrating technology addiction and use: an empirical investigation of online auction users. *Mis Quarterly*, 35, 4 (2011), 1043-1062.

123. Vance, A., Lowry, P.B., and Eggett, D. Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems*, 29, 4 (2013), 263-290.

124. Wallace, K.A. Anonymity. *Ethics and Information Technology*, 1, 1 (1999), 21-31.

125. Wallander, L. 25 years of factorial surveys in sociology: A review. *Social Science Research*, 38, 3 (2009), 505-520.

126. Walsham, G. Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, 4, 2 (1995), 74-81.

127. Weber, R. Editor's Comments. *Mis Quarterly*, 27, 3 (2003), iii-xii.

128. Whetstone, J.T. How virtue fits within business ethics. *Journal of Business Ethics*, 33, 2 (2001), 101-114.

129. Williamson, O. *The economic institutions of capitalism.* New York: Free Press, 1985.

130. Williamson, O.E. Markets and hierarchies: analysis and antitrust implications. New York, NY: Free Press, 1975.

131. Williamson, O.E. Calculativeness, Trust, and Economic Organization. *The Journal of law & economics*, 36, 1 (1993), 453-486.

132. Willison, R., and Warkentin, M. Beyond deterrence: an expanded view of employee computer abuse. *Mis Quarterly*, 37, 1 (2013), 1-20.

133. Workman, M., and Gathegi, J. Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, 58, 2 (2007), 212-222.

134. Zhou, L., Burgoon, J.K., Twitchell, D.P., Qin, T., and Nunamaker Jr, J.F. A comparison of classification methods for predicting deception in computer-mediated communication. *Journal of Management Information Systems*, 20, 4 (2004), 139-166.

135. Zimbardo, P.G. The Human Choice: Individuation, Reason and Order Vs. Deindividuation, Impulse and Chaos. In, Arnold, W.J., and Levine, D., (eds.), *Nebraska symposium on motivation*, Lincoln: University of Nebraska Press., 1970, pp. 237-307.

Appendix A. Instrument and Analysis

Construct	Variable	Measures for each construct
Technological Idealism (IDEAL)	IDEAL1	IT should never be used to psychologically or physically harm another person
	IDEAL2	IT should never be used to threaten the dignity and welfare of another individual
	IDEAL3	Whenever I use IT, I should be concerned about whether the way I use it maintains the dignity and concern of the society.
	IDEAL4	When I use IT, I should make certain my use does not sacrifice the welfare of others.
	IDEAL5	Moral actions using technology should match the ideals of the most "perfect" action.
Technological Relativism (RELA)	RELA1	Questions of what IT use is ethical for everyone can never be resolved since what is moral or immoral is up to the individual.
	RELA2	Morality of any IT use should be judged only on personal standards, and should not be applied to others.
	RELA3	Ethical considerations in using IT are so complex, that individuals should be allowed to formulate their own individual codes.

Attitude toward unethical IT use (ATT)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	ATT1	Carrying out the action would be good.
	ATT2	Carrying out the action would be valuable.
	ATT3	Carrying out the action would be useful.
	ATT4	Carrying out the action would be wise
	ATT5	Carrying out the action would be attractive.
	ATT6	Carrying out the action would be pleasant.
Moral Intensity (MI)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	MI1	I believe that if I undertake this action, the overall harm to others will be high.
	MI2	I believe that if I undertake this action, the likelihood of general harm to others is high.
	MI3	I believe that if I undertake this action, it would harm others in the immediate future.
	MI4	I believe that if I undertake this action, I would harm people close to me
	MI5	I believe that if I undertake this action, others would feel the negative effects very quickly.
Intention of unethical IT use (INTENT)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	INTENT1	If I were to carry out this action, it makes sense for me to do it.
	INTENT2	Depending on the situation, I could carry out this action.
	INTENT3	If I had the opportunity, I would carry out this action
	INTENT4	All things considered, it is likely that I might carry out this action in the future
	INTENT5	All things considered, I expect to carry out this action in the future
	INTENT6	I intend to carry out this action in the future.
Subjective norms (SN)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	SN1	I would have the support of my fellow students if I were to carry out this action
	SN2	My fellow students would want me to carry out this action.
	SN3	My fellow students would prefer me carry out this action
	SN4	My fellow students would themselves have carried out this action if they had been in my place.
	SN5	I would have been able to take help from my friends for carrying out this action.
Perceived Behavioral Control (PBC)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	PBC1	I would feel comfortable doing the act
	PBC2	If I want, I could easily carry out the act
	PBC3	I would be able to carry out the act even if there was no one to show me.
Technological Facilitation (TECHFAC)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	TECHFAC1	I believe that technology enables me to carry out this action
	TECHFAC2	I believe that technology makes it easy for me to carry out this action.
	TECHFAC3	I believe that technology helps me to carry out this action.
General Computer Self Efficacy (GCSE)	GCSE1	I believe I have the ability to remove information from a computer that I no longer need
	GCSE2	I believe that I have the ability to understand common operational problems with a computer
	GCSE3	I believe that I have the ability to use a computer to display or present information in a desired manner
Non-Traceability (TRACE)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	TRACE1	If I carried out this action, I believe that the computer system could not be used to detect my actions
	TRACE2	If I carried out this action, I believe it would not be possible to identify me using the computer system.

	TRACE3	If I carried out this action, I believe that the computer system could not help ascertain that I did the action.
Lack of Punishment Severity (PUNSEV)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	PUNSEV1	If I were caught after committing the action, the punishment would probably not be severe.
	PUNSEV2	If I were caught after committing the action, chances are that the punishment would not be severe
	PUNSEV3	If I were caught after committing the action, the punishment would most likely not be severe
Overall Gain (OGAIN)	Note: Each subject was asked to respond to the following items only with reference to the specific case scenario assigned to him/her.	
	OGAIN1	Overall, if I committed this action, I would gain from this behavior
	OGAIN2	Overall, if I committed this action, I would benefit rather than lose from this behavior
	OGAIN3	Overall, if I committed this action, I would incur more gain than loss from this behavior
	OGAIN4	Overall, if I committed this action, I would profit significantly and suffer little damage from this behavior
Past Unethical IT use	PASTBEHAVIOR	If you have acted in a similar way (as described in the case scenario) before, how many times have you done so? (0, 1-5, 5-10, 10-20, >20)*

Table A1. The Instrument for the study

Psychometric Details

	IDEAL	RELA	MI	ATT	INTENT	PBC	TRACE	GCSE	TECHFAC	PUNSEV	OGAIN	SN
IDEAL	**0.807**											
RELA	-0.054	**0.841**										
MI	0.163	0.059	**0.915**									
ATT	-0.121	0.137	-0.341	**0.825**								
INTENT	-0.138	0.179	-0.412	0.667	**0.875**							
PBC	-0.101	0.043	-0.319	0.265	0.55	**0.902**						
TRACE	-0.123	0.191	-0.119	0.384	0.417	0.128	**0.962**					
GCSE	-0.066	0.014	-0.187	0.095	0.201	0.489	0.006	**0.908**				
TECHFAC	-0.002	-0.057	-0.278	0.202	0.368	0.51	0.045	0.375	**0.941**			
PUNSEV	-0.059	0.071	-0.175	0.459	0.446	0.225	0.342	0.041	0.233	**0.945**		
OGAIN	-0.069	0.172	-0.376	0.668	0.61	0.322	0.417	0.164	0.243	0.455	**0.955**	
SN	-0.078	0.097	-0.416	0.59	0.648	0.343	0.368	0.104	0.322	0.43	0.477	**0.924**

Table A2. Average Variance Extracted
(The diagonal shows square root of AVE; other entries show the correlation between the latent constructs)

Appendix B. Case scenarios

(Note: each scenario represents HI/LO manipulations of the following exogenous variables: moral intensity, lack of punishment severity, and non-traceability. Thus we have a total of 2 X 2 X 2 or 8 case scenarios. The manipulations pertaining to a particular case are also noted beside the case number in parentheses.)

Case 1 (Moral Intensity: HI; Punishment Severity: HI; Traceability: LO)
Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the

database that stores all the grades for this particular course.

As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers.

A possibility strikes you. Since you know the password to the professor's website, you can log in to his website (using your personal laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. You know that the instructor is hardly concerned of security issues and would never imagine that somebody might act in this way. Thus, if you were to commit this action, you would most likely not be caught. However, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for a course taught by a different professor). The student was caught, and he was dismissed from the university.

Case 2 (Moral Intensity: HI; Punishment Severity: HI; Traceability: HI)

Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the database that stores all the grades for this particular course.

As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers.

A possibility strikes you. Since you know the password to the professor's website, you can log in to his website (using your personal laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. However, you know that the professor is very concerned about security issues and has extensive technological controls (e.g. log and audit files) in place to know of all the accesses to his website and his database. You also know that his TA checks the log and audit files once a week in order to verify whether there has been any unauthorized access of the professor's website and the course grade database. Thus, if you were to commit this action, you would most likely be caught. Furthermore, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for the same course taught by the same professor). The student was caught, and he was dismissed from the university.

Case 3 (Moral Intensity: HI; Punishment Severity: LO; Traceability: LO)

Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the database that stores all the grades for this particular course.

As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers.

A possibility strikes you. Since you know the password to the professor's website, you can log in to his website (using your personal laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. You know that the instructor is hardly concerned of security issues and would never imagine that somebody might have acted as you did. Thus, if you were to commit this action, you would most likely not be caught. Furthermore, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for a course taught by a different professor). Though the student was caught, he was let off only with a warning.

Case 4 (Moral Intensity: HI; Punishment Severity: LO; Traceability: HI)

Imagine that you are in your senior year at your university. You have been doing poorly in one of the key courses of your major you are currently taking. You are afraid that your GPA and future prospects will be affected by a bad grade in this course. One day, while you are visiting the office of the course instructor, you accidentally gain access to the password to his website. This website contains the database that stores all the grades for this particular course.

As the semester is drawing to a close, you realize that you are heading toward a very low grade in the course. With companies (intending to hire from your major) scheduled to visit the campus next month, you want to be among the strongest candidates in your class (in terms of the grades). Unfortunately, you know that with your current performance in this course, you will not be perceived by employers as a strong candidate compared to your peers.

A possibility strikes you. Since you know the password to the professor's website, you can log in to his website (using your personal

laptop from home), access the grade database, and actually increase your grades substantially. This will make you a more attractive candidate as compared to the more deserving students from your major. However, you know that the professor is very concerned about security issues and has extensive technological controls (e.g. log and audit files) in place to know of all the accesses to his website and his database. You also know that his TA checks the log and audit files once a week in order to verify whether there has been any unauthorized access of the professor's website and the course grade database. Thus, if you were to commit this action, you would most likely be caught. However, you remember that there was a similar occurrence of unauthorized grade change by a student some years ago (for a course taught by a different professor). Though the student was caught, he was let off only with a warning.

Case 5 (Moral Intensity: LO; Punishment Severity: HI; Traceability: LO)

Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet.

The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. You know that the technical group in charge of the wireless network does not maintain extensive technological controls (e.g. log and audit files) to keep track of all the websites the users (who are connected to the wireless network) are visiting. Neither are there any log or audit files to monitor downloading activities of the users. Thus, if you were to download the songs over the Internet, you would most likely not be caught. However, you know that students who were previously caught downloading music from illegal websites onto their personal computers were severely punished by the university authorities. They were expelled from the dorm and also the university.

Case 6 (Moral Intensity: LO; Punishment Severity: HI; Traceability: HI)

Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet.

The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. However, you know that the technical group in charge of the wireless network maintains extensive technological controls (e.g. log and audit files) that keep track of all the websites the users (who are connected to the wireless network) are visiting. Furthermore, the log and audit files also keep track of the size of the downloads for each user. Since the music files are large, they may easily attract attention of any person monitoring the log files. Thus, if you downloaded the songs over the Internet you would most likely be caught. Furthermore, you know that students who were previously caught downloading music from illegal websites onto their personal computers were severely punished by the university authorities. They were expelled from the dorm and also the university.

Case 7 (Moral Intensity: LO; Punishment Severity: LO; Traceability: LO)

Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet.

The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. You know that the technical group in charge of the wireless network does not maintain any extensive technological controls (e.g. log and audit files) to keep track of all the websites the users (who are connected to the wireless network) are visiting. Neither are there any log or audit files to monitor downloading activities of the users. Thus, if you were to download the songs from the Internet, you would most likely not be caught. Furthermore, you know that students who were previously caught downloading music from illegal websites onto their personal computers were let off only with a warning.

Case 8 (Moral Intensity: LO; Punishment Severity: LO; Traceability: HI)

Assume that you currently live in the university dorm. You have an avid interest in music and closely follow the new music albums being released by a certain artist. One of the albums that you want to possess has just been released. However, it is very expensive and given your limited budget as a student, you do not wish to pay for it. However, you realize it is possible to download the songs of the album from an illegal website onto your personal laptop using the Internet.

The dorm you stay in has hi speed wireless network. You can connect to the wireless network from your laptop. However, you know that the technical group in charge of the wireless network maintains extensive technological controls (e.g. log and audit files) that keep track of all the websites the users (who are connected to the wireless network) are visiting. Furthermore, the log and audit files also keep track of the size of downloads for each user. Since the music files are large, they may easily attract attention of any person monitoring the log files. Thus, if you downloaded the songs from the Internet you would most likely be caught. However, you know that students who were previously caught downloading music from illegal websites onto their personal computers were let off only with a warning.

Appendix C. Results of Non-linear Analysis

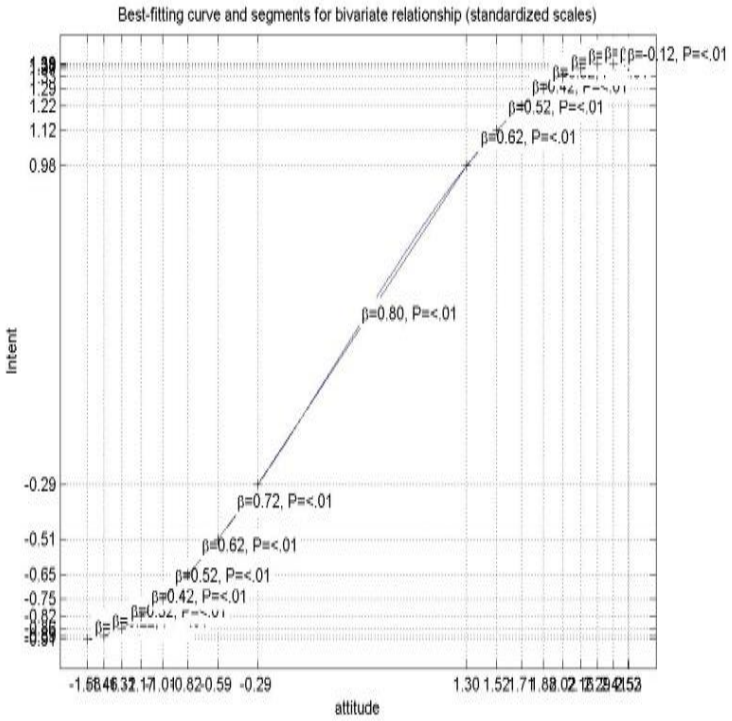

Figure C1. Attitude vs Intention

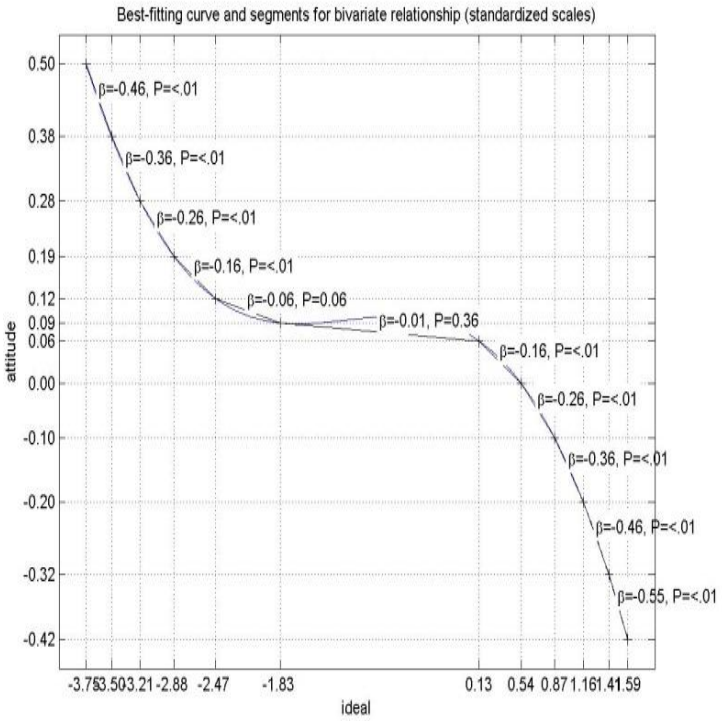

Figure C2. Technological Idealism vs. Attitude

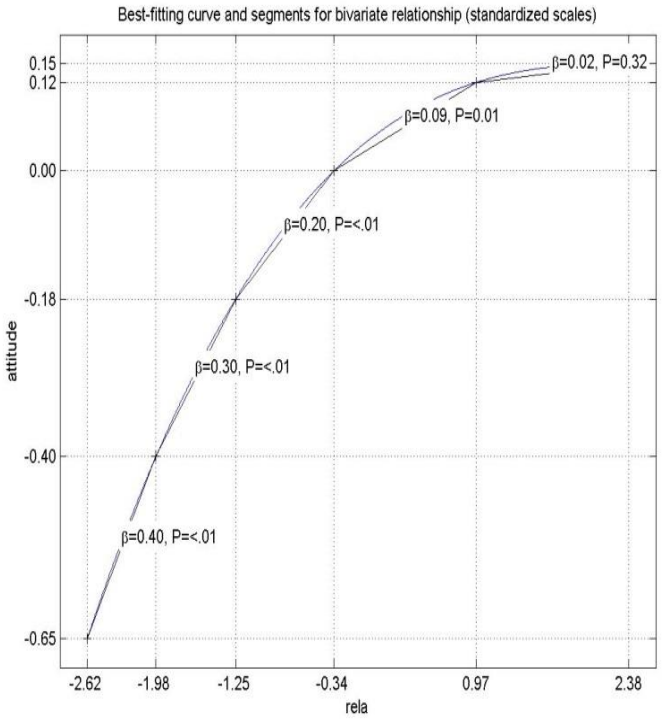

Figure C3. Technological Relativism vs. Attitude toward

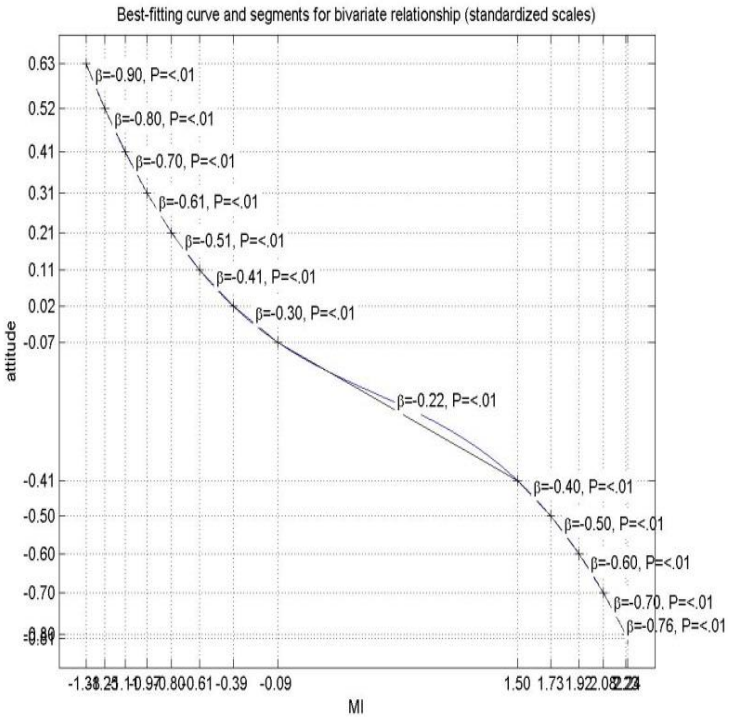

Figure C4. Moral Intensity vs. Attitude toward unethical IT

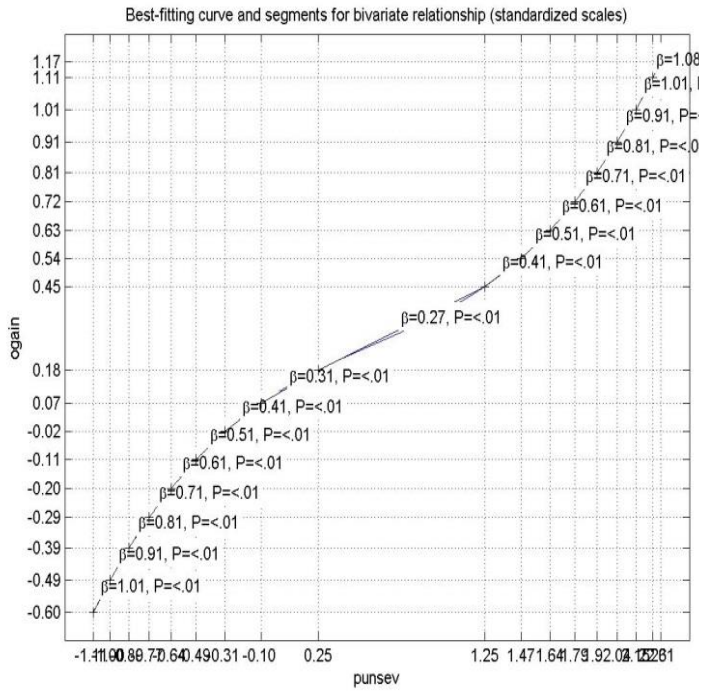

Figure C5. Punishment Severity vs. Overall Gain

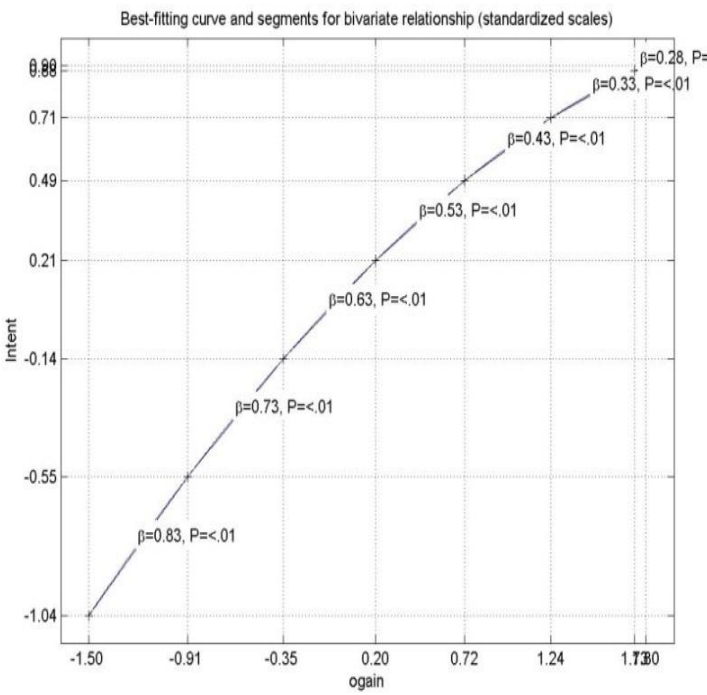

Figure C6. Overall gain vs. Intention

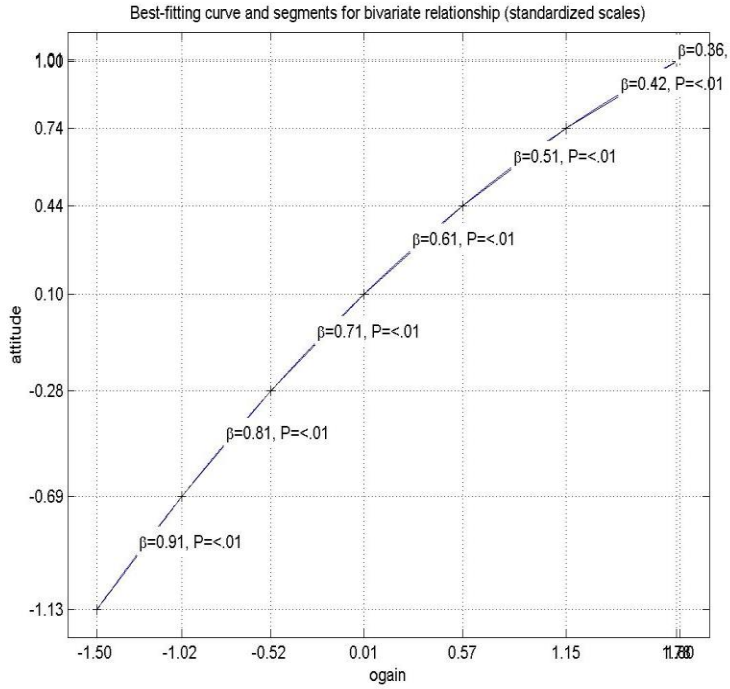

Figure C7. Overall gain vs. attitude

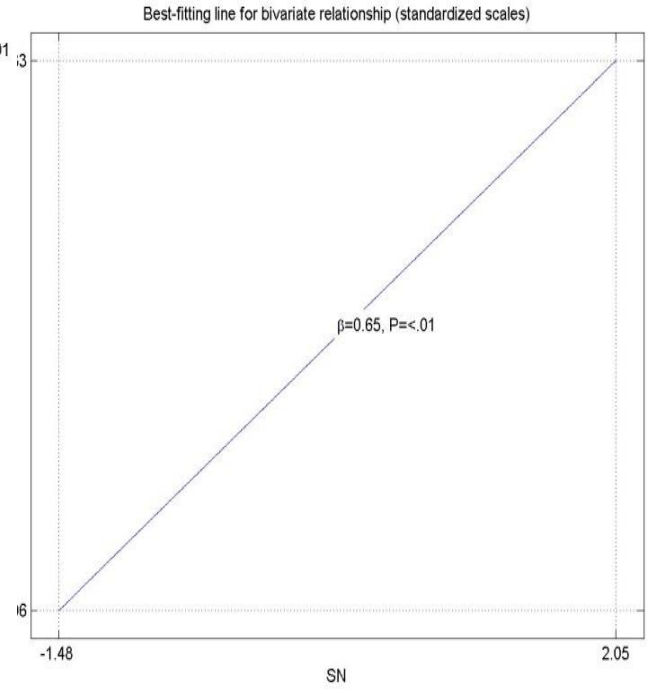

Figure C8. Subjective norms vs. Intention

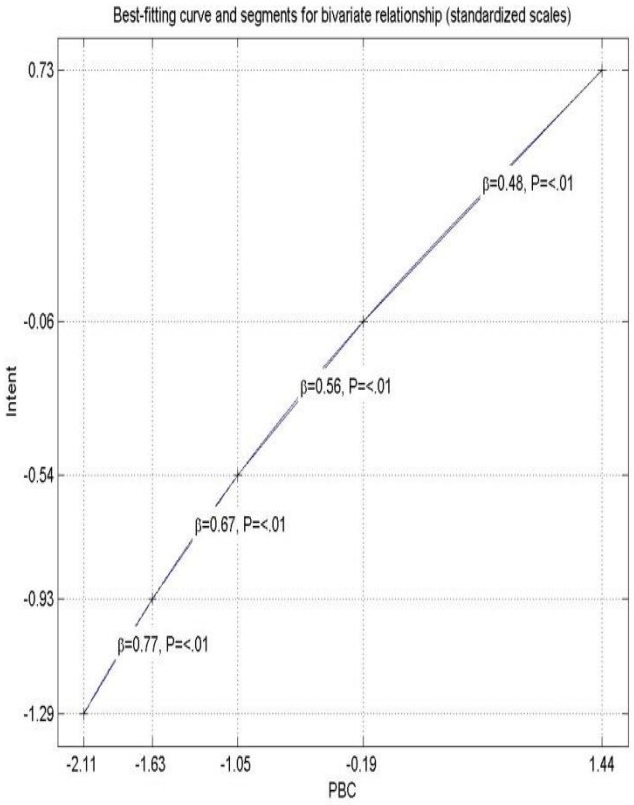

Figure C9. Perceived Behavioral control (PBC) vs. Intention

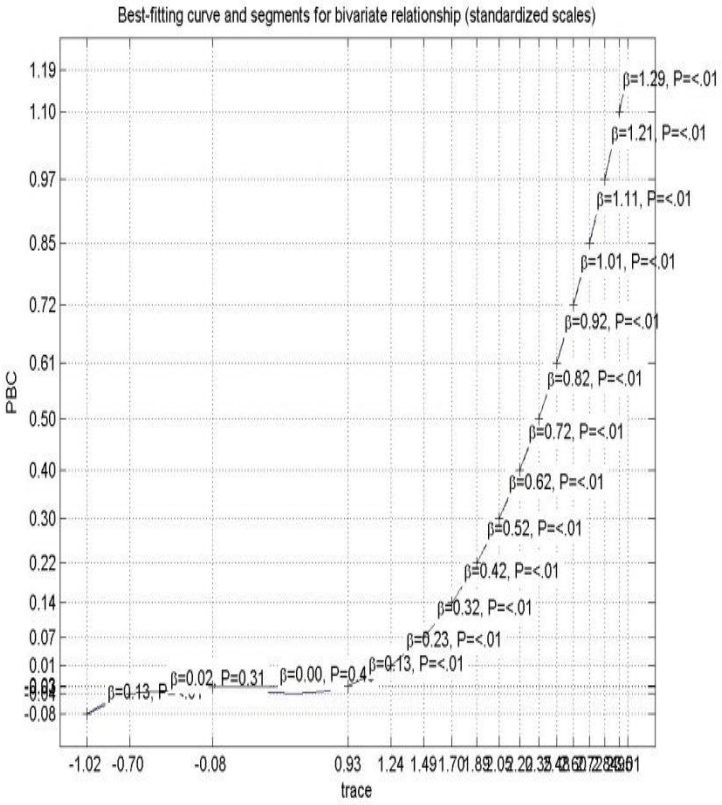

Figure C10. Non-traceability vs. PBC

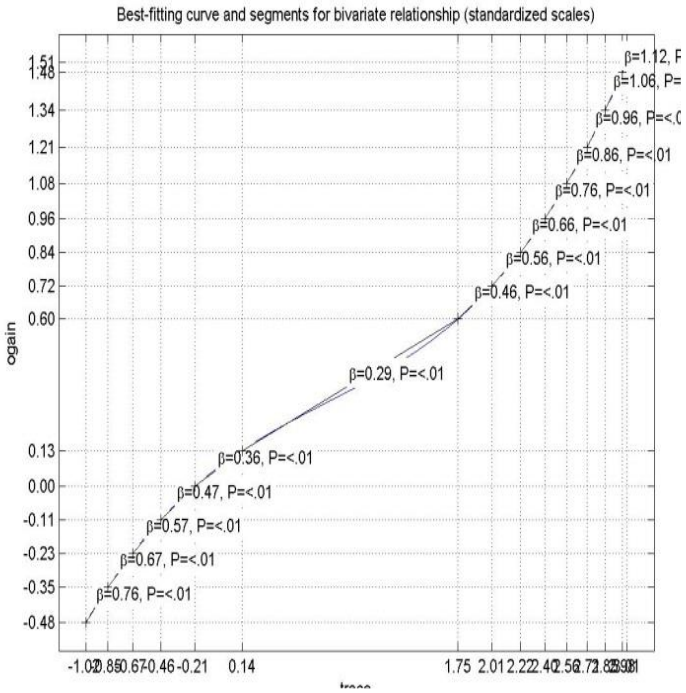

Figure C11. Non-traceability vs. Overall gain

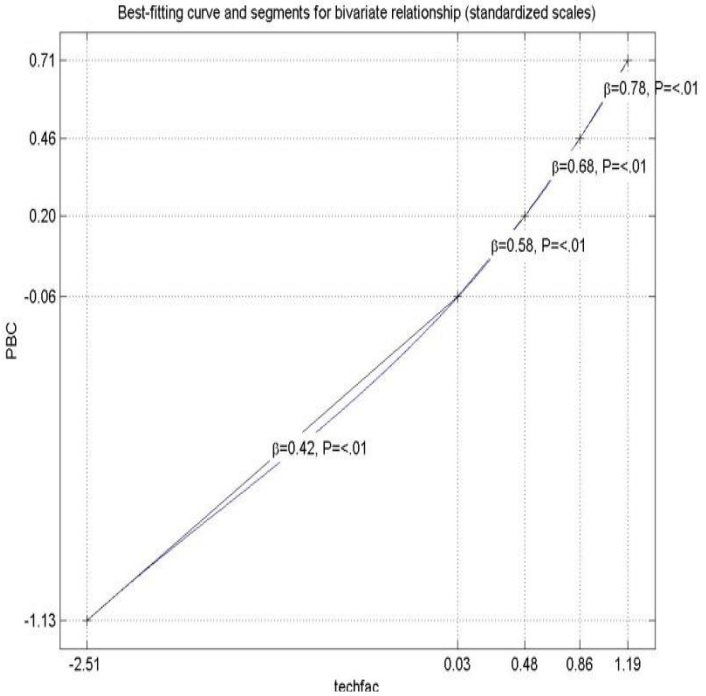

Figure C12. Technological Facilitation vs. PBC

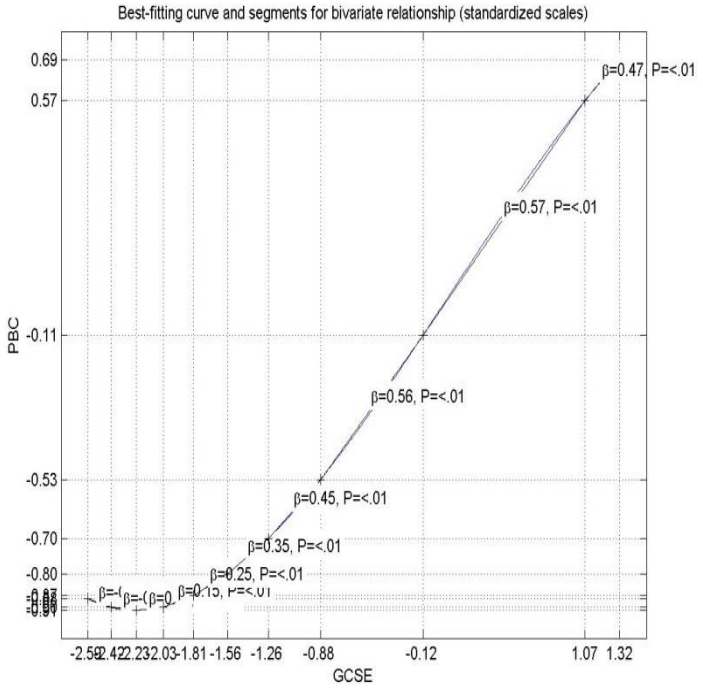

Figure C13. Computer efficacy vs. PBC

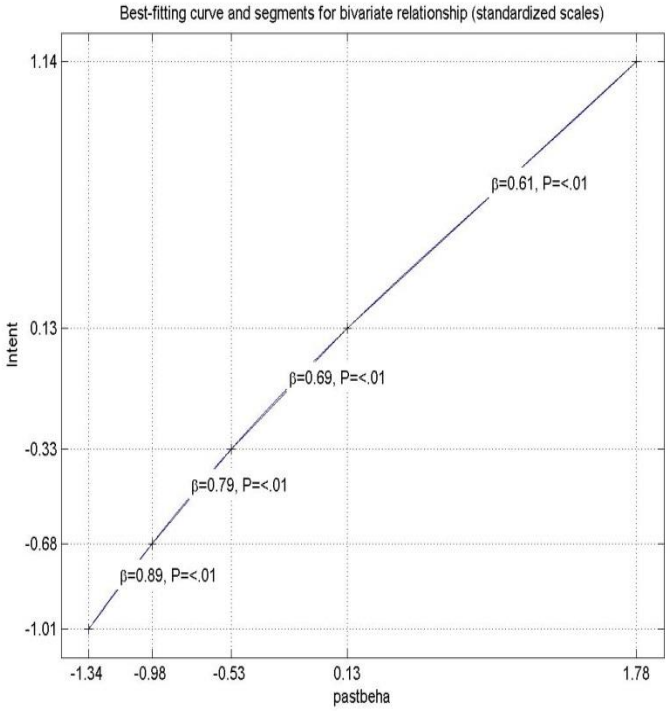

Figure C14. Past Behavior vs. Intention